Does bank's financial standing influence the risk of a cyberattack?

Łukasz Kurowski[1]
SGH Warsaw School of Economics; e-mail: lkurow@sgh.waw.pl
https://orcid.org/0000-0002-3306-4276

Paweł Smaga[2]
SGH Warsaw School of Economics; corresponding author e-mail: psmaga@sgh.waw.pl
https://orcid.org/0000-0003-3913-0833

Corresponding author address:

SGH Warsaw School of Economics

al. Niepodległości 162

02-554 Warsaw, Poland

phone: +48 22 564 60 00

Total word count (after requested revisions): 16 344

[1] Associate professor
[2] Associate professor

Abstract

The aim of this article is to identify the financial determinants of cyberattacks on banks, using a global sample of 319 publicly disclosed cyberattacks that occurred in 53 countries between 2014 and 2024. Drawing on data on bank-level financial ratios, we find that the size of a bank (its total assets and deposit base), as well as its total capital ratio, are positively associated with the likelihood of experiencing a cyberattack. Doubling the bank's assets raises the probability of a cyberattack by approx. 3.8 pp. The results are robust across various model specifications, estimation methods and samples. Nevertheless, in the US, smaller, less resilient, and less efficient banks are more likely to experience observed cyber incidents. Overall, the findings have actionable policy implications for both banks and prudential supervisors.

Keywords: cyber risk, financial stability, hackers, bank, DDoS, ICT

Subject classification codes: F50, G00, G21, H56, K24

Funding

This work was supported by the funding from the Collegium of Management and Finance at the SGH Warsaw School of Economics (Poland) under grant number KZiF/S25:1.50.

1. Introduction

The visible increase in recent decades in the frequency of cyberattacks on banks, their complexity and the magnitude of losses is the result of several factors [1], including accelerating digital transformation of banking operations (incl. cloud computing, third-party services), the surge of the Internet of Things, remote work, as well as cyber warfare and the rise of AI-driven systems, all of which contribute to greater importance of cyber security for banks. Numerous industry reports (e.g. by F5 Labs, NTT and ENISA) regularly indicate that the financial services sector and banks are among the prime targets of cyberattacks and highly exposed to cyber risks. Additionally, [2] noted that nearly one-fifth of all cyber incidents affect firms from the financial sector, with banks accounting for around half of these incidents. [3] notes that for EU banks the share of operational risk capital requirements (which includes cyber risk) in total capital requirements has been gradually growing over the years, currently amounting to circa 13% (as of June 2025), with operational risk capital requirements constituting the second most important component of banks' risk-weighted assets, following credit risk. In the banking union, the number of cyberattacks and reported significant cyber incidents increased considerably in recent years, with ransomware attacks on service providers soaring and DDoS attacks remaining the most prevalent type of incident reported by banks in the banking union [4], all of which gives justification of cyber risk in banks as a worthy area of scientific study.

The rapidly growing importance of cyber risk in banks is in stark contrast to the underdevelopment of studies on this topic. Cyber risk is emerging as one of the most critical risks in modern banking [5, 6], although it differs from "traditional" economic banking risks (e.g., like credit risk). Its sources, transmission mechanism and consequences are far from identified and thoroughly researched. Furthermore, the sources of data on cyberattacks are rarely publicly available, and usually fragmented, unstructured and often not updated, posing a challenge for empirical assessment of this phenomenon [7]. With this paper we wish to contribute to partially filling this gap by advancing the work on the first phase in the NIST framework ("Identify") in the context of banks.

The literature on cyberattacks in financial institutions is relatively nascent but began to rapidly grow in recent years. A literature review by [8] revealed that a cybersecurity landscape in the financial sector that is both dynamic and complex, therefore resilient defense in financial institutions hinges on a blend of cutting-edge technical measures, strong cultural underpinnings, and well-orchestrated incident response protocols. A similar review by [9] identified the main types of attack vectors, vulnerabilities they exploit, and potential countermeasures banks should undertake.

The main aim of the paper is therefore to identify the financial determinants of cyberattacks on banks, as observed in publicly disclosed data, by empirically exploring which aspects of bank's financial standing are linked to a higher likelihood of experiencing such events. We ask the question why are hackers more likely to attack some banks than others? We investigate the issue on a wider cross-country sample of 281 banks, subject to 319 publicly disclosed cyberattacks worldwide in 53 countries in the years 2014 to 2024. To estimate the likelihood of cyberattacks on banks, we apply a nonlinear panel framework using the Conditional Mixed Process (CMP) estimator [10], which accommodates both binary dependent variables and endogeneity among regressors. This approach enables the simultaneous estimation of a system of equations, where key financial variables—such as profitability, liquidity and bank size—are treated as potentially endogenous and instrumented via their own lags.

To address data limitations, we adopt two complementary empirical approaches. The first relies on within-bank variation over time among banks that experienced at least one cyberattack, allowing us to examine when cyberattacks occur within already targeted institutions. The second approach uses a broader cross-sectional dataset including banks without recorded cyberattacks, capturing differences

across institutions while acknowledging that the absence of disclosed events does not necessarily imply the absence of actual cyberattacks.

We extend this literature in several dimensions, for example, by considering a larger set of banks, and by examining the role of a potentially wider set of bank-level characteristics in explaining the likelihood of occurrence of cyberattacks. Most studies to date only focus on the determinants of cyberattacks on corporations (see e.g. [11]), while it is important to also study this issue on a sample of banks. Since banks are institutions of public trust, playing a key role in the economy and exhibiting high interconnectedness, the consequences of a successful cyberattack would be significantly more severe and widespread than in the case of a typical corporation. This study thus focuses on cyberattacks on commercial banks - such approach compliments recent studies exploring importance of cyberattacks on insurance [12, 13] and central banks [14], all of which are distinctly different financial institutions from commercial banks.

We differ from the limited existing research on determinants of cyberattacks on banks (see [15] and [2]) by using a global (not just US) sample, exploring the issue depending on the country of bank's operation and hacker type, and using alternative measures of bank's profitability, resilience, and liquidity. Such approach makes our results more robust and - to our knowledge - has not yet been applied in the literature. This contrasts with other studies, treating cyberattacks as "0-1" variables, i.e., without distinguishing among different features of attacks or subsamples. Further, we adopt an alternative approach to [16], who measured disclosure intensity of cyber risk in banks using a text-mining method (of banks' annual 10-K filings), as we use the data on materialized, publicly disclosed cyberattacks. Moreover, most studies focus only on the US sample - [8] identified that in similar studies on cyber risk in financial institutions, geographic focus was indeed still skewed towards developed markets, leaving questions about the transferability of these findings to emerging economies. Our sample remedies this by including cyberattacks from banks in emerging countries as well.

Our approach is closest to [17] who on the sample of US banks explored the predictive power of bank characteristics and cybersecurity ratings for signaling realized cyber incidents. Yet we apply different econometric framework, analyze cyberattacks not cyber incidents (thus excluding internal IT failures without malicious human intent), and investigate the predictive power of twice as many micro- and macro variables than [17], and use a global sample. We also follow the approach of [18] who attempted to better understand what factors drive the differences in the extent to which banks were targeted by cyberattackers using financial malware (Zeus). We join their pursuit to enrich the hitherto little empirical work done into the underlying reasons why certain targets are selected more often than others.

Having found the significant importance of larger bank size (measured using total assets and the deposit base) in increasing the likelihood of cyberattacks, we thus contribute to the debate on potential drivers of cyberattacks from the perspective of hackers (see [6]). However, the results point to important heterogeneities when assessing predictive strength bank variables when controlling for particular features of attacks. Consequently, our results are relevant for policymakers, supervisors and bank managers when managing cyber risk and increasing the cyber resilience of the banking sector.

This paper is structured as follows. First, we review the literature on cyber risk in banks to identify the research gap and propose a research hypothesis. Next, the paper explains the structure of data on cyberattacks and how we linked it with financial data. We also clarify the adopted methodology. Then, we elaborate and discuss the results, including robustness checks. The concluding section summarizes the findings and outlines policy implications.

2. Literature review

The paper attempts to contribute to the literature on the importance of cyber risk in finance, specifically focusing on determinants of cyberattacks. While there is already a growing amount of literature

exploring the cyberattacks on corporations, much less attention is paid to studies on cyberattacks on commercial banks.

We begin by clarifying the cyber terminology used. According to NIST, a cybersecurity event is a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). A narrower category is a cyber incident defined as an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Cyber incidents are a result of two types of triggers – an unintentional malfunction of the IT infrastructure or a malicious act of a determined actor – and in this paper we focus on the latter, i.e., cyberattacks. For the purpose of this study, we adopt the definition of cyberattack as a deliberate, hostile action by a threat actor intended to compromise systems, data, or IT services. Such attacks can result in significant damage to both physical and intangible assets, disrupt business operations, or harm an organization's reputation. Therefore, *ex definitione* a cyberattack initially impairs three elements in banks: it compromises data integrity, makes data and IT systems unavailable, and breaches data confidentiality. To sum up, as a rule of thumb, classification of those terms can follow the following sequence: 1) is the occurrence observable? – a cyber event; 2) does it jeopardize CIA triad or violate policy? – a cyber incident; 3) is there evidence of external actor with deliberate malicious intent – a cyberattack.

At the same time, cyber risk can be defined as a combination of the probability of cyber incidents and their potential impact on the condition of a banking, which can occur via financial losses, operational outages, or the contagion of risk to other sectors [19]. In line with high-level causal model of cyber risk by [20], the threat exploits existing exposure to perform harm, the degree of which is mitigated by security measures. In the context of this model, given the data constraints, we attempt to identify which features of the bank cause the threat (cyberattacker) to enact harm. Yet, measuring these abstract variables is challenging in practice, as e.g. no single indicator captures the sum of preventive and reactive measures across an organization’s technology, processes and people.

As previously mentioned, cyberattacks are becoming more frequent, more cost-effective to execute (partly due to advances in AI), and increasingly sophisticated and targeted, making them difficult to detect and assess [21, 22]. Hacker attacks can be targeted at banks themselves, but also at the third-party providers of services used by banks (such as cloud services), creating potential vulnerabilities. Cyberattacks differ from traditional risks (e.g., credit, liquidity risks) in the banking sector, as they propagate faster and their determinants are bound by economic, technical and social aspects. Furthermore, the resilience to cyber risk is not measured in terms of stock of capital or liquid assets but rather is a derivative of the quality of IT infrastructure and the qualifications of IT staff.

The limited research on cyber risk in banks focuses almost exclusively on the potential consequences of cyber incidents, incl. cyberattacks. Most cyber risk losses are small, although some have a low frequency and a high impact, i.e., fat-tailed distribution [5, 23], accounting for up to a third of total operational VaR in commercial banks [24]. Consequences of a cyber incident often include (although hard to estimate precisely) reputational damage, legal costs, fall in customer trust, reduced profits, and heightened liquidity risks [16, 25, 26, 27], leading to negative stock market reactions [28, 29, 30]. [31] estimated that the average cost of cyber incidents for banks and insurers would be the equivalent of 2-3% of their annual profits, with a 5% VaR possibility that such costs would exceed 25-34% thereof. Unfortunately, most costs (esp. indirect ones) are difficult to quantify, and therefore likely to be underestimated due to the unavailability of comprehensive and robust data. Losses from a cyberattack might even impact loan loss provisions and ultimately also NPLs [15, 32]. [33], [34] and [35] provide empirical evidence that banks experience a significant decline in deposits following a successful cyberattack (a phenomenon often referred to as a “cyber run”). [32] additionally shows that in response to cyberattacks banks collect fewer deposits, are less profitable, and lend less, but [35] show that they can also lend more to compensate for the losses after data breaches. This is in line with a simulation by

[36], arguing that a prolonged cyber incident in banks leads to confidence shock and triggers stressed liquidity outflows. Cyber threats also raise the likelihood of bank defaults, especially among banks facing deposit outflows, although those with ample liquidity buffers are less affected [37]. According to [38], cyber risk loss rates have a U-shaped relationship with bank size in the US, i.e. are higher for both smaller and bigger banks. Moreover, they evidence that more profitable and efficient US banks have lower cyber loss rates. The indicated studies thus provide clear evidence of the severe negative financial consequences of a successful cyberattack on banks, with potentially systemic consequences.

The ECB defines cyber resilience as the ability to protect electronic data and systems from cyberattacks, and to resume business operations quickly in the event of a successful cyberattack. Banks that invest more in IT, are bigger and hold large reserves of high-quality liquid assets tend to exhibit stronger cyber resilience, and can endure, recover from, and adapt to cyber-induced shocks [6, 34, 39]. [40] indicate that implementing cybersecurity policies (to increase cyber resilience) in banks leads not only to improved financial resilience but also has a statistically significant positive effect on profitability measures.

The impact of a cyberattack is often not limited to the victimized bank but can propagate on a systemic scale when the initial shock is amplified [41], causing cascading cyber failures [42]. The impact thereof on financial stability is monitored via three contagion channels [43, 44]: (i) the operational working of key economic functions and the transmission of any outage to other banks, (ii) the size of financial losses (in connection with the duration of any long-term outage of key economic functions), and (iii) the loss of confidence in the banking system. [45] integrate cybersecurity risk into the theoretical model of bank runs (e.g., [46]) and show that cyberattacks on the five most active US banks can generate significant spillovers to other banks. In this context, [47] found that the systemic consequences of a successful cyberattack via payment system channel are higher when markets are more volatile and when financial intermediaries' balance sheets are strained. Still, what is missing in the literature is a holistic assessment of cyber vulnerabilities across different types of financial institutions, allowing for identification of systemic vulnerabilities. First attempts in this regard include study by [48], identifying market sentiment, particularly fear triggered by cyber incidents, as a key channel amplifying the contagion of cyber risk across financial sectors. Also [49] propose to use of a Leontief "input-output" table to calculate the multiplier effect of losses from cyberattacks, considering not only direct losses but also secondary effects that can affect the entire economic chain from production to consumption.

The studies on cyberattack consequences provide the backbone for the construction of nascent systems to monitor and measure cyber risk exposure in banks and banking systems [50]. [51] propose a cyber stress testing methodology and simulate that the end-of-day bank liquidity risk is most severe when a cyberattack hits a major bank or several banks simultaneously through dependence on a common critical service provider. In this framework, it is assumed that the cyberattack on a bank causes a temporary unavailability of processing the payment transaction system, leading to liquidity pressure not only in a victimized bank, but also leading to systemic consequences. A similar exercise was conducted by [36], who assessed the liquidity position of the banks that do not receive payments and are put under severe stress because of a cyberattack on one of the interconnected banks, necessitating ample provision of liquidity into the payment system. The payment system interlinkages, augmented with financial data from banking reporting systems, can also feed into a cyber map - a quantitative tool covering the key technologies, services and external service providers, and their connections with financial sector institutions, allowing for identification of critical nodes/services in the system [43, 52]. Nevertheless, an IMF survey shows that the development of cyber maps among supervisors is still in its infancy [53]. The reviewed studies and cyber stress test methodologies thus imply that the consequences of a cyberattack, at least in the short term, might be akin to an acute liquidity shock, resulting from temporary unavailability of bank (payment) services.

Unfortunately, while studies exploring the consequences of cyberattacks on banks are emerging, very few focus on their determinants. Cyberattacks in the financial sector are inevitable, yet the perceived

irregularity of their timing and attack vectors makes them difficult to anticipate or explain holistically. The propensity of an attack is likely driven not only by micro-level characteristics, but also by country-level features such as increasing geopolitical tension, higher digitalization, higher banking market concentration, and lesser quality of cyber regulations and IT infrastructure [2]. In contrast to the studies analyzed above, we assess the potential drivers of cyberattacks on banks to contribute to filling this gap. Based on a US corporate sample, [54] found that a positive tone of annual reports (10-K filings) has a significant and positive association with the odds of a data breach, which is linked to strong financial performance and promising prospects. Also, [55] explored this issue using a text-based measure of exposure to cybersecurity risk on the basis of corporate 10-K reports, indicating that firms are more likely to experience a future cyberattack if they have higher cybersecurity risk scores, and are of a larger size and younger age. In a similar vein, [56] used text-mining on quarterly earnings calls, finding that cyber-exposed corporations are likely to be large and with a high share of intangible assets, high liquidity and cash flow ratios, and growth opportunities. Moreover, [29], also on a corporate sample, discovered that larger, more profitable and older firms, with better visibility are more likely to experience a cyberattack. Moreover, the findings of [11] show that adoption of digital technologies, in particular cloud computing and ecommerce platforms due to their payment functionality, is a crucial channel that expands the attack surfaces of corporates in Italy, thereby elevating their vulnerability to cyberattacks. Similarly, [6] show that the cost of a cyberattack is positively correlated with corporate firm size, while [15] found that US bank data breaches are determined, among others, by asset quality, profitability and resilience measures, as well as the bank's size.

We test the validity of some of these conclusions on a global banking sample and study the role of financial determinants of cyberattacks. Based on the literature review, we therefore propose the following hypothesis:

H1: *An increase in bank size is associated with a higher likelihood of observed cyberattacks.*

With H1, we aim to explore both the existence of statistical significance, as well as the sign of the coefficient.

3. Data and methodology

We constructed two databases (A and B), each used for different types of modeling but consisting of data on i) characteristics of cyberattacks on banks, ii) their financial condition, and iii) the macroeconomic variables. The following section explains how data was carefully procured and curated.

3.1. Data on cyberattacks

We attempted to find as many publicly reported cyberattacks on banks as possible. There is lack of a precise definition or taxonomy of cyberattacks, and the few available open-source databases on cyberattacks are rarely updated and often limited in scope [57]. Various niche repositories, news sites, and blogs catalog cyberattacks, particularly those involving banks, but the data is often poorly structured, inconsistently coded, and not updated. Unfortunately, these databases often lack information on the severity of the attack or estimates of cyber losses resulting from the cyberattack, which is why we could not include these aspects in our analysis. Given the unique nature of each cyberattack, caution is advised in comparative analyses thereof. The prime reasons for the limited data availability on cyberattacks include banks' unwillingness to disclose cyberattacks and the fragmented disclosure frameworks. Ultimately, we constructed our sample by merging input from two open source cyberattack databases with comparable structures.

To create database A, we first used the "CISSM Cyber Events Database"[3] as created by the Center for International and Security Studies at Maryland and GoTech [58, 59]. This dataset contains structured information on cyberattacks along with their different features. We extracted the cyberattacks on commercial banks from the section "industry: code 52" labeled „Finance and Insurance" after curation of data. The CISSM covers attacks from 01.01.2014 to 15.10.2024. Next, we utilized the European Repository of Cyber Incidents (EuRepoC) database[4], an independent research consortium dedicated to providing evidence-based scientific analysis of cyber incidents. From this database we filtered out data only on cyberattacks on commercial banks from the section "Critical infrastructure: Finance" under "Receiver subcategory". The EuRepoC sample includes attacks from 01.01.2005 to 31.03.2025.

Similarly to [14, 60], we extracted the following characteristics of cyberattacks from both databases:

- Date – year of attack
- Location – country in which the bank-victim operates
- Victim – a bank targeted in the cyberattack
- Actor Location – (suspected) country of the hackers
- Actor – name of the hacker group responsible for the attack
- Actor type – variable indicating the nature of the actor responsible for the cyberattack:
    - Criminal – an organization that illicitly accesses networks for financial gain
    - Hacktivist – an individual or group acting due to social or political motives
- Motive - the intended results sought by the actor committing the cyberattack
    - Protest – the disruption of services to send a political or social message to the target organization, or to a government or population indirectly.
    - Sabotage – the intentional, irreparable destruction of information, networks, or devices
    - Financial – exfiltrating sensitive data for direct or indirect financial gain.
- Attack type – variable indicating whether the primary result of the cyberattack was disruptive, exploitative, or a mixture of the two.
    - Disruptive – impedes the target organization's normal operations
    - Exploitive – illicitly accesses or exfiltrates sensitive information such as personal identifiable information, classified information, or financial data.
    - Mixed – incorporates both disruptive and exploitative elements, such as a ransomware attack.

We then curated the data from those two databases by excluding records of cyberattacks where the name of the targeted bank was not disclosed. We also merged the classifications of cyberattack type and motive in these two databases to ensure comparability, before eliminating any duplicate entries found. Moreover, the number of attacks by actor type "Nation-State" on commercial banks (when the name of the victim was disclosed) was very miniscule in both databases, which unfortunately prevented us from including this actor type in the models. Furthermore, if a single bank was attacked more than once in the same year – it was counted as one case, but attacks on the same bank in different years were counted as separate cases. In most cases, a bank was targeted only once, which aligns with the distribution of the number of cyberattacks per company in all economic sectors [23]. However, we acknowledge the imperfections of the data sources used, as cyber databases significantly underreport the number of cyberattacks, including only those acts that were successful and publicly disclosed, disregarding also the majority of unsuccessful, often unreported attempts – [1] estimates that over 40 percent of cyber incidents may remain undisclosed. Consequently, we were able to gather data only on disclosed cyberattacks, as only bank supervisors have access to confidential data on all cyber incidents in banks. Unfortunately, we were unable to obtain them. However, this issue is encountered in any external

[3] The database is available at: https://cissm.umd.edu/research-impact/publications/cyber-events-database-home
[4] The database is available at: https://eurepoc.eu/dashboard

database with data on cyberattacks, constructed on the basis of public information. Therefore, such limitations warrant careful interpretation of results.

Following these adjustments, we obtained a sample of 281 commercial banks, subject to 319 cyberattacks worldwide in 53 countries, which occurred in the years 2014 to 2024 in database A.

Database B is a derivative of database A, covering only banks with cyberattacks that occurred in 2023, which is the most "numerous" year, covering around one third (112 out of 319) attacks in the full sample. Next, we added 2021-2023 financial data for all banks operating in a country with at least a single bank attacked in 2023. After that, to avoid endogeneity issues, we removed from the list banks that experienced attacks in 2021 or 2022, an approach that is akin to [29], who also classified firms in the sample into targets and nontargets. Ultimately, we constructed database B covering 18 countries with 12 824 banks, 108 of which experienced a reported cyberattack in 2023, with corresponding micro- and macro-level data.

While the use of two datasets allows us to tackle the research problem from different perspectives, each approach is nevertheless subject to limitations, warranting careful interpretation of results. In particular, Database A is restricted to banks that have experienced at least one cyber incident and therefore does not include institutions that were never attacked during the sample period. Therefore, this design does not allow us to identify what distinguishes attacked from non-attacked banks but rather focuses on the timing of incidents within already targeted institutions. Conversely, Database B includes banks which have not experienced a cyberattack and enables cross-sectional comparisons. However, it relies on publicly disclosed incidents, which introduces potential reporting and disclosure biases, as the absence of disclosed attacks does not necessarily imply their absence altogether. In sum, these limitations imply that our results should be interpreted as identifying the determinants of observed cyber incidents under different empirical perspectives, rather than the underlying probability of being targeted per se.

3.2. Bank-level and macroeconomic data

Commercial banks play a central role in the economy, by financing economic growth through the provision of credit. Their financial intermediary role is possible, as banks channel funds gathered from savers to borrowers - banks mainly fund credits from deposits collected from households and corporations. Therefore, it is essential that cyberattacks do not undermine banks' financial condition and disrupt the provision of banking services. In banking practice, a well-established set of financial indicators is used to evaluate the soundness of such financial institutions, which motivates our selection of variables. The selection of bank-level indicators reflects standard approaches used by regulators, central banks and financial institutions to assess commercial banks' standing and risk profile. In particular, bank size captures the scale of bank operations and its systemic importance – bigger banks attract more attention, potentially also from hackers. Profitability measures reflect financial performance and efficiency, as more profitable banks might entice more cyberattacks. Capital and leverage ratios are commonly used to assess bank's resilience to shocks and size of capital buffers – more stable banks might be viewed as more prominent targets by hackers. At the same time liquidity indicators capture bank's ability to withstand short-term funding stress – disclosure of a cyberattack might results in a cyber run on bank's deposits. In the context of cyber risk, shocks to such measures of bank's condition may arise from operational disruptions, financial losses or reputational damage following a cyberattack.

Both databases A and B include annual bank-level data collected from the renowned Orbis database provided by Moody's Analytics, which offers reliable and comparable data from financial statements submitted by banks. For banks that were subject to a cyberattack, we matched the data on the characteristics of the attack with the bank's financial condition ratios. The extracted categories included data from the balance sheet (in thousands of USD), and financial ratios (as percentages). The selection of extracted categories was based on typical values and ratios used in bank financial condition assessments by researchers, central banks, and international financial institutions. The selection of bank-

level indicators was also limited by their availability in the Orbis database. A broader range of ratios was extracted to identify commonalities in banks' conditions that cyber perpetrators could use as a guide when selecting their targets (see Table 1). The collected measures include those assessing the size of the bank, its deposit base, resilience to shocks, profitability, leverage, efficiency, business model, and liquidity risk. We additionally included the country where the bank mainly (or its headquarters) operated, as well as its specialization, i.e., the business model – a commercial or cooperative (incl. savings) bank. Unfortunately, prevalent data gaps in the Orbis database made it impossible to include credit risk metrics, e.g., the NPL ratio in modeling (see [15]). In Table 1, we additionally indicate the expected sign of the given financial ratio and link the reasons behind its inclusion to the results of the literature review (including studies on corporate samples), where available. Ultimately, we follow the structure of ratios like the ones used to study cyber risk in banks by [37], [40], and [16]. A similar, although more limited, selection of ratios was used by [61] to evaluate the impact of digitalization on a bank's operational and cyber risk, and by [62] to proxy the stability-enhancing effect of cyber expenditure in banks.

Table 1. Bank-level and macroeconomic data

Group	Data category	Abbreviation	Description	Expected impact on the probability of a cyberattack	Related literature
Nominal positions					
Size	Total assets	ln_TA	Measure of bank's size and its importance in the economy	Increase	[2, 29, 33, 55, 56]
	Total customer deposits	ln_DEP	Measure of bank's deposit base		[2, 33, 34, 36, 37]
Financial condition ratios					
Profitability	Return on average equity (ROAE) (%)	ROE	Measure of bank's profitability	Increase	[29, 33, 40, 54]
	Net interest margin (average total earning assets) (%)	NIM			
	Cost-to-income (Efficiency) ratio (%)	C_I	Measure of bank's efficiency		
Resilience	Total capital adequacy ratio (%)	TCR	Measure of bank's resilience to shocks	Decrease	[37, 40]
	Total equity / Total assets (%)	LEV	Measure of bank's leverage and resilience		
Liquidity	Loans & advances to customers / Total assets (%)	L_TA	Measure of bank's liquidity and business model	Increase	[37]
	Liquid assets / Deposits & short-term funding (%)	LIQ	Measure of bank's liquidity risk		
Macroeconomic control variables					
Macro	Inflation	CPI	Measure of price dynamics	Increase	
	GDP per capita	GDPpc	Measure of economic growth and country level of development		[1]

Source: own work

We also use macroeconomic control variables. Sources of macroeconomic annual data for countries with a victimized bank include the World Bank (World Development Indicators) and the IMF (World Economic Outlook database) for GDP per capita as well as inflation (consumer prices). Any missing data points were supplemented by data available from national central banks and national statistical offices. We additionally attributed the countries in the sample to either advanced economies or emerging and developing economies, in line with the country classification used by the IMF in the World Economic Outlook Database (as of April 2023). This is inspired by the results of [1], who conducted an in depth assessment of the trends of cyber incidents between countries at different stages of development, having found that developing countries account for approximately 30 percent of the world's publicly disclosed cyber incidents, and that a developing country that reduces its number of major disclosed cyber incidents from the top to the bottom quartile of the distribution could boost its GDP per capita.

Given the international scope of our dataset — which includes banks operating in diverse regulatory environments, economic conditions, and financial systems — we expect substantial heterogeneity in bank characteristics. Such heterogeneity naturally leads to the presence of extreme values in key financial indicators, which may reflect structural differences rather than noise or error.

To reduce the undue influence of such extreme observations and ensure that our regression results are not driven by a handful of outliers, we apply winsorization of bank-level variables at the 1st and 99th percentile levels, allowing us to retain the full sample while mitigating the distorting effects of outliers, resulting in more robust and generalizable estimates. Importantly, this transformation preserves the underlying variation in bank financial profiles, which is essential for identifying meaningful patterns in cyberattack determinants. The descriptive statistics for database A are in Table 2, and for database B in the Annex.

Table 2. Descriptive statistics (database A)

Variable	Obs.	Mean	Std. Dev.
ln_TA	3,802	15.988	2.631
ln_DEP	3,779	15.530	2.645
ROE	3,774	8.751	11.837
NIM	3,760	3.414	2.215
C_I	3,751	64.548	21.525
TCR	2,862	17.661	9.399
LEV	3,762	10.349	5.402
L_TA	3,754	58.636	17.020
LIQ	3,756	35.584	23.011
ln_GDPpc	3,938	10.018	1.259
CPI	3,974	4.408	6.438

Source: own work

3.3 Methodology

In empirical research, causal relationships between economic variables are typically analyzed using econometric models, which allow researchers to identify and quantify statistical dependencies in the data. However, the choice of an appropriate model to be used must first and foremost reflect the specific characteristics of the data and the underlying economic relationships. For example, some variables may influence each other simultaneously, making it difficult to disentangle causes from effects. For example, while financial characteristics of a bank may affect the likelihood of a cyberattack, cyberattacks may at the same time also impact a bank's financial performance. In addition, the nature of the data (e.g., whether the dependent variable is binary or continuous) further determines the selection of appropriate modeling approach. Moreover, the panel structure of the data (i.e., repeated observations for the same banks over time) requires methods that account for differences across institutions. Data limitations are also an important consideration—for instance, further disaggregation of cyberattacks by specific actor types (e.g., state-sponsored actors or hobbyists) would result in very small subsamples, reducing statistical power and leading to unreliable estimates. Therefore, selecting an econometric framework that accounts for these features is essential for obtaining reliable and meaningful results.

To investigate the determinants of cyberattacks on banks in publicly disclosed data, we estimate a series of nonlinear panel models using the Conditional Mixed Process (CMP) estimator developed by [10]. The CMP framework is particularly well suited for our context, where the dependent variable is binary (indicating the occurrence of a cyberattack in a given year) and several of the explanatory variables - including profitability measures (ROE, NIM and C_I), liquidity (LIQ), and the level of deposits (ln_DEP) - are likely to be endogenous.

Given the significant risk of reverse causality in this context — for instance, not only might bank's profitability or liquidity affect its likelihood of experiencing a disclosed cyberattack but cyberattacks themselves also impact a bank's financial performance and its liquidity — it is essential to explicitly account for endogeneity in the estimation strategy. We also treat the volume of deposits as an endogenous variable, following the approach of [63], who highlight that cyberattacks may trigger deposit withdrawals, particularly in smaller or more vulnerable banks. The CMP estimator allows for simultaneous estimation of multiple equations while accounting for potential correlation of unobserved error terms across equations, thus providing consistent parameter estimates in the presence of endogeneity.

Specifically, we estimate a recursive system in which the primary equation models the probability of a cyberattack as a function of a set of bank-level and macroeconomic covariates, simultaneously modeling the potentially endogenous regressors - ROE, NIM, C/I, LIQ, ln_DEP - in auxiliary equations, each modeled as a function of their own first and second lags. These lagged terms act as internal instruments, a widely accepted and standard approach in dynamic panel models to mitigate endogeneity [64, 65].

The multiequation CMP model used in the analysis assumes that the dependent latent variable y_{it}^{*} (e.g., the probability of a cyberattack) is a function of a vector of financial variables F_{it} and macroeconomic variables M_{tc}, along with fixed effects α_i. Since some financial variables $Z_{it} \subset F_{it}$ are endogenous, the model includes their corresponding instrumental equations with instruments W_{it}, which consist of lagged values of these variables. The entire system is estimated simultaneously, allowing for a correlation between error terms and proper identification of parameters.

Formally, the model can be expressed as:

$$\begin{cases} y_{it}^{*} = F_{it}\beta_F + M_{tc}\beta_M + \alpha_i + \varepsilon_{it} \\ Z_{it} = W_{it}\gamma + u_{it} \end{cases} \quad (1)$$

where:

y_{it}^{*} is the latent dependent variable (probability of a cyberattack) for bank *i* at time *t*,
F_{it} is a vector of financial variables for bank *i* at time *t*,
M_{tc} is a vector of macroeconomic variables at time t and country c
$Z_{it} \subset F_{it}$ denotes the subset of endogenous financial variables,
W_{it} are instruments (lagged values of Z_{it}),
α_i are bank fixed effects,
ε_{it} and u_{it} are error terms that may be correlated.

All models control for bank-specific unobserved heterogeneity using fixed effects and include key bank financial variables and macroeconomic conditions (GDP per capita and inflation). Estimations are conducted using robust standard errors clustered at the bank level. The use of CMP is especially advantageous given the nonlinear and recursive nature of the data-generating process, as well as the combination of binary and continuous variables within the model system.

Each estimated equation (denoted as Eq) incorporates a distinct combination of the bank's financial variables (see Table 3). This approach avoids including highly correlated financial measures that capture similar aspects of the bank's financial condition within the same model (the correlation matrix is presented in Figure 1), which helps to mitigate multicollinearity and ensure more reliable parameter estimates.

Table 3. Combination of bank's financial variables in each estimated equation

	Bank size		Profitability			Resilience		Liquidity		Macro-control	
	ln_TA	ln_DEP	ROE	NIM	C/I	TCR	LEV	L_TA	LIQ	CPI	ln_GDPpc
Eq1	x		x			x		x		x	x
Eq2	x		x				x	x		x	x
Eq3		x	x			x		x		x	x
Eq4		x	x				x		x	x	x
Eq5	x			x		x			x	x	x
Eq6	x			x			x		x	x	x
Eq7		x		x		x		x		x	x
Eq8		x		x			x	x		x	x
Eq9	x				x	x		x		x	x
Eq10	x				x		x		x	x	x
Eq11		x			x	x			x	x	x
Eq12		x			x		x		x	x	x

Source: own work.

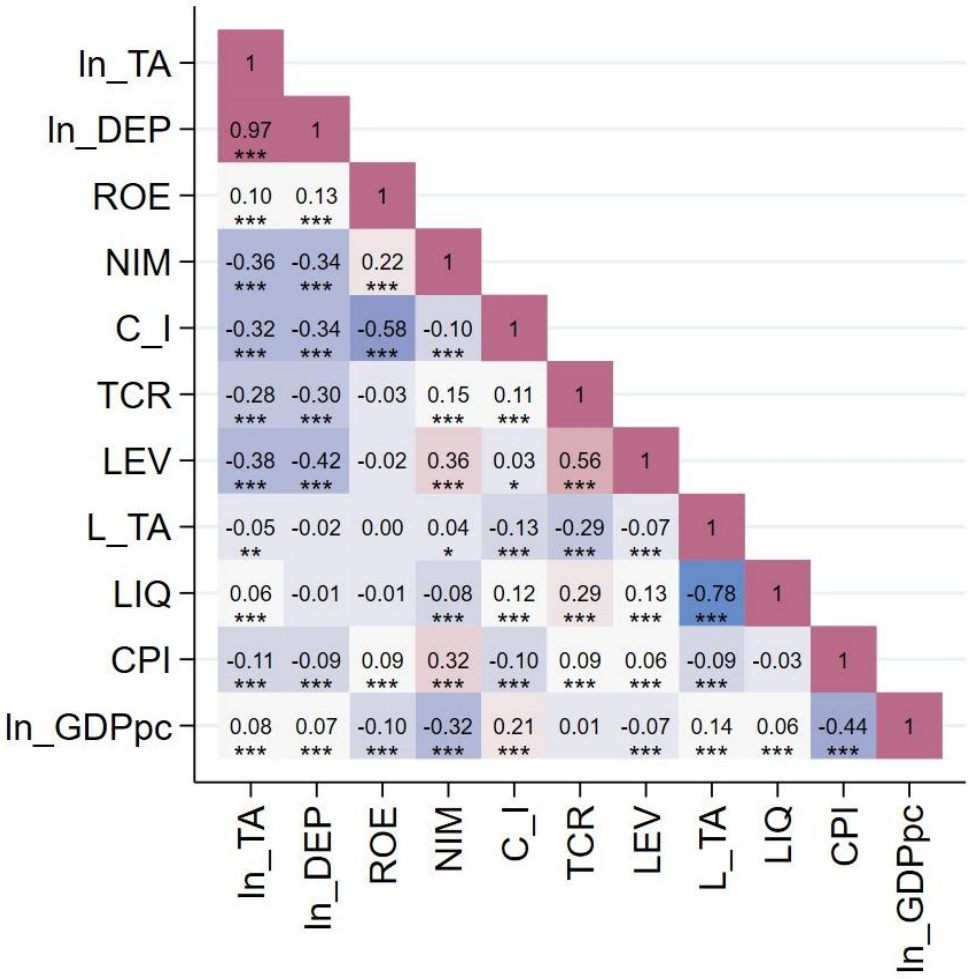


Figure 1 Correlation of the independent variables used in the model

Source: own work.

Alt text: A chart showing how strongly the variables are related to each other – darker colors indicate stronger relationships

As a robustness check, we complement our panel data models with a cross-sectional analysis focused exclusively on the year 2023 using database B. In this setup, we construct a dataset comprising two groups of banks: (i) banks that experienced a cyberattack in 2023, and (ii) a matched group of banks that did not report any cyberattack, which enables the assessment of whether the core relationships identified in the panel regressions using database A also hold in a single-year setting that includes a counterfactual group.

To model the probability of a cyberattack occurrence, we estimate a series of logistic regressions where the dependent variable is a binary indicator equal to 1 in the case of a bank attacked in 2023, and 0 otherwise. The explanatory variables include same measures as in the panel approach. Additionally, we use both contemporaneous values (t) and lagged values (t−1 and t−2) of the regressors to test the robustness of the results to timing assumptions.

The general form of the estimated model can be represented as follows:

$$\Pr(Cyber\_attack, 2023 = 1) = logit^{-1}(\beta_0 + \beta_1 F_{i,2023} + \beta_2 M_{c,2023} + \varepsilon_i) \qquad (2)$$

$$\Pr(Cyber\_attack, 2023 = 1) = logit^{-1}(\beta_0 + \beta_1 F_{i,2022} + \beta_2 M_{c,2023} + \varepsilon_i) \quad (3)$$

$$\Pr(Cyber\_attack, 2023 = 1) = logit^{-1}(\beta_0 + \beta_1 F_{i,2021} + \beta_2 M_{c,2023} + \varepsilon_i) \quad (4)$$

Equations (2), (3), and (4) differ in the temporal structure of the financial variables included, with equation (2) assessing the influence of financial indicators from the year of the cyberattack (contemporaneous values), equation (3) incorporating lagged financial variables from one year prior to the attack, and equation (4) considering variables lagged by two years. Such an approach examines whether the timing of financial conditions relative to the attack date has any predictive power regarding the likelihood of a cyberattack.

The model closest to ours is that of the [2], who examined drivers of cyber incidents using a probit regression. A similar approach was also proposed by [15] to explore determinants of cyberattacks on banks. However, our study addresses endogeneity, uses a more recent sample built from multiple cyberattack databases, and focuses specifically on banks, along with analyzing a broader set of bank-level financial ratios as potential determinants of cyberattacks.

Unfortunately, data constraints prohibited us from including any measures of banks' cyber resilience as independent variables. All three databases we used (CISSM, EuRepoC, Orbis) contain no data on preventive cybersecurity policies or countermeasures taken after the attack on a given bank. This can be seen as limitation in our methodology, hopefully remedied in the future as more detailed data on cyberattacks becomes available.

4. Results and discussion

4.1. Insights from data on cyberattacks

Based on database A, we draw several conclusions. The number of reported cyberattacks by both criminals and hacktivists remained relatively stable from 2014 until a sharp surge in 2023, which was primarily driven by higher criminal activity and proliferation of cyber warfare between Ukraine and Russia. There is very high correlation between the actor type, their motive and cyberattack type – on average criminals with financial motives cause exploitive attacks, while hacktivists motivated by protest mainly aim to disrupt a bank's operations. Attacks on commercial banks constitute the majority of the sample (84%), while cooperative (incl. savings) banks were attacked much less often (16%), which prohibited us from estimating the models separately for both types of banks, given the insufficient number of attacks on cooperative (incl. savings) banks, which would not provide reliable estimations. Commercial banks were almost to the same extent victims of both disruptive (42%) and exploitive (45%) attacks, and attacked in all countries in the sample, which in contrast to cooperative banks, which suffer mainly from exploitative attacks (62%). This observation leads to our focus only on the actor type when analyzing panel modeling results further i.e. attacks by criminals vs hacktivists. Criminals mostly attack commercial banks, but also to some extent cooperative ones, while hacktivists almost exclusively target commercial banks.

The actor country remains undetermined in two-thirds of cases (63%), while among those attributed, hackers stem mostly from Russia, Ukraine and Brazil. While almost half (43%) of the actors remain unidentified, the rest is quite fragmented. The most prominent actors include "NoName057(16)" and "Anonymous" (hacktivist groups attacking mainly commercial banks), as well as the financially motivated criminal gang "Cl0p", which attacks both commercial and cooperative banks. This means that we were unable to produce estimations separately for different variants of actor country and actor name.

4.2. Estimation results

The baseline results were achieved using database A (see Table 4). The nature of the data and the structure of database A determined the presentation of panel modeling results. As Database A includes

only banks with at least one publicly disclosed cyberattack, the analysis relies on within-bank variation over time and should be interpreted as explaining when cyberattacks occur, rather than which banks are targeted. Due to the very high similarity of results between those for actor type, motive, and cyberattack type, we focus on analyzing the results for actor type and don't report on the results for the other two dimensions[5]. This means that the results for attacks motivated financially are very close to those perpetrated by criminals, while attacks intended as a protest are very similar to those done by hacktivists. Ultimately, we analyze and discuss the results in the following dimensions:

- the baseline model on the whole sample;
- models for attacks on US banks vs non-US banks;
- models for attacks on banks operating in advanced economies vs emerging and developing economies;
- models for attacks by criminals and by hacktivists separately.

This approach allows for a more nuanced understanding of the heterogeneity in the impact of cyberattacks across attacker types and geographic regions, in contrast to the hitherto literature. When providing the interpretation of results, we indicated the potential financial mechanisms behind them, but most importantly based on literature review and market intelligence we attempt to map the results with potential motives for attacks from "inside a hacker's mindset". For the purpose of interpretation, we focus on those variables for which the coefficients were found significant only in the majority of model specifications.

[5] The results are available upon request from the authors.

Table 4. Results for the full sample – the baseline model (database A)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.0678***	0.0428**	0.0467***	0.0229*	0.0676***	0.0437***	0.0449***	0.0248**	0.0645***	0.0433**	0.0438***	0.0234**
	(0.0164)	(0.0134)	(0.0118)	(0.0090)	(0.0165)	(0.0132)	(0.0117)	(0.0089)	(0.0167)	(0.0135)	(0.0120)	(0.0090)
Profitability measure (estimations)	-0.0005	-0.0001	-0.0007	0.0001	0.0043	0.0047	0.0027	0.0044	-0.0002	0.0001	-0.0001	-0.0000
	(0.0006)	(0.0005)	(0.0006)	(0.0005)	(0.0054)	(0.0044)	(0.0053)	(0.0045)	(0.0004)	(0.0004)	(0.0004)	(0.0004)
Resilience measure (estimations)	0.0026*	-0.0024	0.0027*	-0.0023	0.0027*	-0.0028	0.0025*	-0.0030	0.0025*	-0.0024	0.0028*	-0.0025
	(0.0011)	(0.0018)	(0.0011)	(0.0018)	(0.0012)	(0.0018)	(0.0011)	(0.0018)	(0.0011)	(0.0018)	(0.0012)	(0.0018)
Liquidity measure (estimations)	-0.0004	-0.0005	-0.0004	-0.0004	-0.0006	-0.0005	-0.0003	-0.0005	-0.0004	-0.0005	-0.0005	-0.0004
	(0.0007)	(0.0006)	(0.0007)	(0.0004)	(0.0005)	(0.0004)	(0.0007)	(0.0006)	(0.0007)	(0.0004)	(0.0005)	(0.0004)
CPI	0.0038***	0.0046***	0.0038***	0.0045***	0.0036**	0.0043***	0.0038***	0.0045***	0.0037**	0.0044***	0.0036**	0.0045***
	(0.0011)	(0.0010)	(0.0011)	(0.0010)	(0.0011)	(0.0010)	(0.0011)	(0.0010)	(0.0011)	(0.0010)	(0.0011)	(0.0010)
ln_GDPpc	0.2125***	0.2814***	0.2391***	0.3068***	0.2050***	0.2694***	0.2334***	0.2989***	0.2111***	0.2728***	0.2369***	0.3016***
	(0.0405)	(0.0341)	(0.0379)	(0.0309)	(0.0409)	(0.0341)	(0.0382)	(0.0310)	(0.0405)	(0.0340)	(0.0378)	(0.0308)
Fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	2697	3538	2697	3534	2689	3548	2700	3552	2699	3547	2688	3547

Note: Standard errors in parentheses, * p<0.05, ** p<0.01, *** p<0.001

Baseline model

The results for the full sample (see Table 4) indicate that bank size, measured by total assets and deposit base, is consistently associated with a higher likelihood of cyberattacks within already affected banks. ln_TA has consistently been found to be significant in all 12 model specifications. The coefficients are positive, indicating that in general larger banks are more likely to experience cyberattacks.

The bigger the bank becomes, the more complex IT systems it uses and thus more potential weak points in the IT infrastructure may emerge – a larger attack surface for a hacker. Furthermore, many large banks still rely on legacy systems that are difficult to update, incompatible with modern IT security protocols, and thus more vulnerable to exploitation [66, 67]. Bigger banks are additionally more valuable targets, as they hold larger pools of personal, financial, and transactional data of millions of customers, which is highly valuable on the dark web. Large banks also face significant regulatory scrutiny and might experience challenges in implementing uniform protections across all their extensive operations. Similarly, bigger banks, while capable of significant recovery efforts, may likewise be hampered by the scale of operations making them slower and less able to respond [18]. Our results additionally confirm the anecdotal evidence from hacking websites that select their victims among the biggest, most famous and most visible banks, making them attractive targets for hacktivists, which want to send as strong political a signal as possible by targeting the largest banks, which will be widely covered in the media.

Still, the results about the importance of bank size have to be interpreted in caution. Most of regulatory reporting/disclosure requirements for cyber incidents in major jurisdictions world-wide are binding for: the biggest banks, listed banks (so usually the largest ones) or banks with assets size above a certain materiality threshold (so usually medium-sized and larger ones). This is because regulators treat bigger banks as higher-impact entities for financial stability, consumer protection, and market transparency. Size and systemic importance of the bank materially change how reporting rules apply in practice - larger banks face faster timelines, more detailed requirements, and higher supervisory scrutiny. The positive coefficient on size may therefore partially reflect determinants of regulatory disclosure rather than determinants of targeting by hackers.

Our results are similar to those revealed on a corporate sample by [6, 29, 55, 56], and on a banking sample by [15], also suggesting that the size of the victimized entity increases the risk of a cyberattack. We likewise provide ground for the cybermapping approach proposed by [43], who in an interconnected banking network defines each entity as a node, with regard to its importance to the system by means of indicators such as, for example, total assets. We additionally validate the findings of the study by [2], who on a global sample of financial institutions also empirically identified the size as a key determinant of the probability of experiencing a cyber incident. Also, [17] provide data showing that the biggest banks are the ones with the highest percentage of experiencing at least one cyber incident, 2017-2025, among all asset size categories. In line with our results, they indicate that realized incidents are disproportionately concentrated among the largest banks, consistent with their greater digital complexity and visibility to attackers and with the key role of size in attacker incentives.

Comparable conclusions can be drawn for the size of a bank's deposit base (ln_DEP) in the baseline model, as it was also found significant with a positive sign, the same as ln_TA, which is due to a very high correlation between ln_TA and ln_DEP in our sample, and in general in the banking sector. From the perspective of hackers, banks with a larger deposit base "have more money that can be stolen" and thus become more attractive targets for criminals with financial motives. However, our insights are dissimilar to those by [18], who uncovered that Zeus attack intensity on online banking services during 2009-2013Q1 were weakly correlated with level of bank deposits in the US, suggesting that there are other factors driving target attractiveness than merely the size of bank or its customer base. Such discrepancy might be the result of us having a wider sample (in terms of geography and timespan) and including attacks not only by financially motivated cybercriminals.

Next, we computed the marginal effects for each bank-level variable, with the results shown in Figure 2.

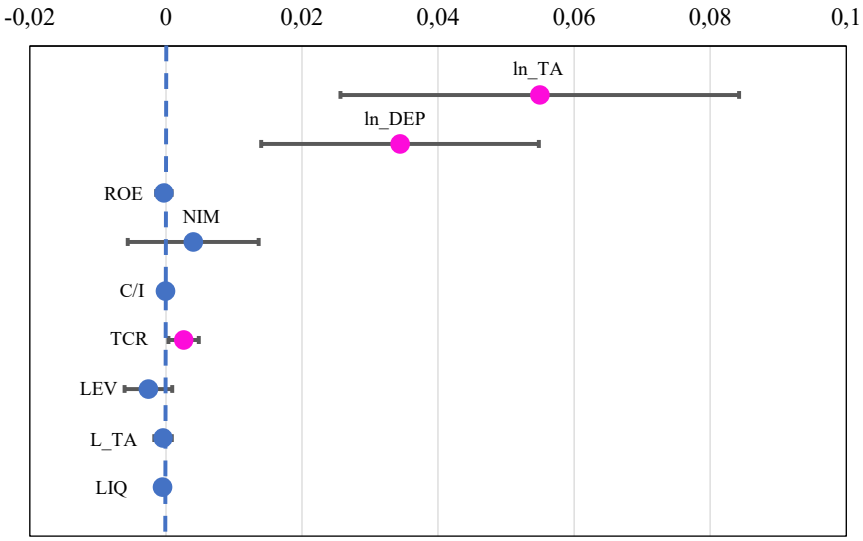


Figure 2 Marginal effects of bank-level variables (database A)

Note**:** The figure displays average marginal effects from nonlinear panel models predicting a cyberattack. The positive values indicate a greater likelihood of cyberattack, while the error bars represent 95% confidence intervals, and the red markers denote statistically significant predictors at the 5% level. Each effect represents the average marginal effect estimated across separate models (corresponding results are presented in Table 4).

Source: own work.

Alt text: Points show the estimated effect of each variable on the likelihood of a cyberattack – values further to the right indicate a higher probability. Horizontal lines show the uncertainty range around each estimate.

According to the marginal effects presented in Figure 2, larger banks (i.e., those with higher total assets and deposit bases) are more likely to experience cyberattacks: a one-unit increase in ln_TA is associated with an increase in the probability of experiencing a cyberattack by approximately 5.5 percentage points. In other words, converting logarithmic values into actual asset sizes indicates that a 100% rise in assets is associated with an increase in the probability of a cyberattack by approximately 3.8 percentage points. A similar, though smaller, effect is observed for ln_DEP. Both variables capturing bank size are statistically significant.

Moreover, inspired by [37] and [38], we attempted to investigate the issue of potential non-linearity (or U-shaped relationship) in the impact of ln_TA by adding ln_TA^2 as an explanatory variable. However, the coefficients of ln_TA^2 were insignificant (see Table 5). This result compliments the findings of [38] who showed that there is a U-shaped relationship between a US bank size and its cyber risk losses.

Table 5. Estimation results for the nonlinear effect of bank asset size (database A)

	(1)	(2)	(3)	(4)	(5)	(6)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Profitability measure	ROE	ROE	NIM	NIM	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	LIQ	LIQ	L_TA	LIQ
ln_TA	0.0669***	0.0450**	0.0678***	0.0474***	0.0644***	0.0466***
	(0.0172)	(0.0138)	(0.0173)	(0.0137)	(0.0174)	(0.0139)
ln_TA^2	-0.0006	0.0016	0.0001	0.0026	-0.0001	0.0024
	(0.0033)	(0.0026)	(0.0032)	(0.0026)	(0.0032)	(0.0026)
Profitability measure (estimations)	-0.0005	-0.0000	0.0043	0.0049	-0.0002	0.0000
	(0.0006)	(0.0005)	(0.0054)	(0.0044)	(0.0004)	(0.0004)
Resilience measure (estimations)	0.0027*	-0.0027	0.0027*	-0.0032	0.0026*	-0.0027
	(0.0012)	(0.0018)	(0.0012)	(0.0018)	(0.0011)	(0.0018)
Liquidity measure (estimations)	-0.0004	-0.0005	-0.0006	-0.0005	-0.0004	-0.0005
	(0.0007)	(0.0006)	(0.0005)	(0.0004)	(0.0007)	(0.0004)
CPI	0.0038***	0.0045***	0.0036**	0.0042***	0.0037**	0.0043***
	(0.0011)	(0.0010)	(0.0011)	(0.0010)	(0.0011)	(0.0010)
ln_GDPpc	0.2127***	0.2821***	0.2049***	0.2704***	0.2111***	0.2741***
	(0.0405)	(0.0341)	(0.0409)	(0.0341)	(0.0405)	(0.0341)
Fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
N	2697	3538	2689	3548	2699	3547

Note: Standard errors in parentheses, * p<0.05, ** p<0.01, *** p<0.001

Source: own work.

As for the macroeconomic indicators, both measures of economic growth p.c. (ln_GDPpc) and inflation (CPI)[6] have significant and positive signs (see Table 4), indicating that cyberattacks are more likely to be observed in more affluent countries and in periods of higher inflation. One possible interpretation is that higher levels of economic development are associated with more sizable banking sectors and larger volumes of savings held within them, which may make them more attractive targets for cyber criminals. At the same time, higher inflation reflects periods of economic or social instability and turmoil, which could be associated with an increased frequency of cyberattacks, including those with non-financial motives, like hacktivists.

At the same time, the results of the baseline model for the full sample (see Table 4) indicate that the variables measuring bank's resilience (LEV), profitability and liquidity are not significant. Notwithstanding, TCR in all 6 model specifications has been found to be significant, with banks with higher TCR able to withstand more losses and shocks, and generally considered more stable. Thus, hackers might consider such banks as a more ambitious hacking challenge, making a successful attack much more satisfying and earning more esteem in the dark web. We also cannot exclude the existence of a "more bank capital = more money to steal" hacker mindset.

The graphical summary of the results of attack models on US vs non-US banks, advanced vs emerging and developing economies, and criminals vs hacktivists is presented in Figure 3. Detailed results of the estimates can be found in the respective tables in the Appendix.

[6] Model specifications with the official interest rate instead of inflation rate generally provided the same results.

Figure 3 The estimated coefficients for bank-specific variables across different groups of models

Note: The estimated parameter value represents the average of the estimated parameters for a given variable across different model specifications. The model specifications are analogous to those presented in Table 4. Bars outlined in red indicate variables that are statistically significant at the 5% level (p-value < 0.05). Source: own work

Alt text: Bar charts showing the estimated effects of selected variables - positive (negative) values indicate a higher (lower) likelihood of a cyberattack.

US banks vs non-US banks

Out of 319 attacks in the sample, one third occurred in US banks, while the rest were reported in much smaller numbers in banks functioning in Ukraine, Russia, Italy, Portugal, India and others. Such proportions are close to the results of [5], as well as [1], who on a comparable global sample to ours (from 2014 to 2023) identified US, Russian Federation, UK, India and Ukraine among the top five targeted countries, by number of disclosed cyberattacks in sector finance and insurance. This incentivized us to model the results separately for US and non-US banks. We divided the sample into attacks on US banks and non-US banks also because of more developed reporting requirements for cyberattacks in the US, which could explain the high representation of US banks in the full sample. Estimated results for US banks and non-US banks are in Appendix.

As presented in Figure 3, the results for non-US banks are in line with the baseline model, i.e., significant positive coefficients for ln_TA, ln_DEP and TCR. Other independent variables were insignificant.

As for US banks specifically, we unearth several interesting results in contrast to non-US banks. Both ROE and C_I have significant coefficients with negative and positive signs, respectively. Thus, lower profitability and efficiency (higher C_I and lower ROE) are associated with a higher likelihood of cyberattacks. Banks with higher C_I often have a lot of operational inefficiencies in internal processes and may have fewer resources available to invest in robust cybersecurity measures. Less profitable banks are under financial stress and thus might prioritize immediate financial concerns over long-term investments in cybersecurity, which are often quite costly, which can, in turn, lead to them having outdated or insufficient cyber security measures. This pattern may be consistent with the interpretation that banks with weaker financial performance have lower operational capacity or fewer resources available for cybersecurity, which could be associated with more attack surface and weaker defense policies. Such an interpretation is in line with the negative and significant coefficient for LEV (share of equity to total assets) in US banks – exemplifying overall that a less resilient US bank is more vulnerable to a cyberattack. In the case of ln_TA and ln_DEP, the coefficients are statistically significant but negative—an opposite pattern to the baseline model—indicating that, in the US sample, cyberattacks are more likely to be observed in smaller banks.

Overall, the determinants of cyberattacks are different in the US than in other countries. In the US, hackers target mainly smaller, less resilient and inefficient banks, confirming the “easy prey strategy” [60]. Those results are in line with findings of [16], who also on a sample of US banks revealed that smaller banks, institutions with lower financial stability, higher operational costs, and are more affected by cyber risk in terms of weakening their strategic position. However, our findings are inconsistent with estimations of [17], who reveal that bank size and balance sheet composition - particularly total assets, deposits-to-assets, and loans-to-assets - are among the most consistent predictors of cyber incidents in US banks. Still, they apply external cybersecurity ratings to quantify each bank’s external security posture and use random forest models as primary modeling approach. Contrastingly, we employ realized cyberattacks within the panel modeling framework, which might explain the divergence in results.

Overall, the pattern we observed for US banks and the contrasting results with other studies may result from data gaps and reflect differences in disclosure regimes, regulatory reporting requirements, and the overall relatively higher visibility of cyber incidents in the US compared to other countries.

Advanced economies vs emerging and developing economies

Almost two thirds of attacks occurred in advanced (61%), while less than half (39%) in emerging and developing economies. Criminals were more than twice as active in advanced than in emerging and developing economies, based on publicly disclosed cyberattacks, while hacktivists more or less equally targeted banks operating in both types of countries. These proportions are in line with the global statistics of cyber incidents in all economic sectors [1]. On average, banks attacked in advanced economies were five times bigger than those attacked in emerging economies, which is due to the structure and different

level of development of the banking systems in these two groups of countries. Estimated results for these groups of countries are in the Appendix.

As shown in Figure 3, for banks in emerging economies, the estimation results are similar to those of the baseline model - the growth in bank size influences the propensity of a cyberattack (ln_TA and ln_DEP are significant and positive), but the positive effect of TCR is no longer present. While ROE appears significant with negative sign half of the models, this inconsistency prevents us from interpreting it as evidence of a true underlying relationship.

This contrasts with the results for banks in advanced economies, where ln_TA and ln_DEP are no longer statistically significant. This means that in advanced economies, even smaller banks must implement robust security measures, making banks of all sizes generally more difficult targets for potential hackers. This might imply that hackers targeting banks specifically in advanced economies might be driven by other, non-financial features. Advanced economies have competitive cybersecurity markets, and peer pressure and more robust regulatory frameworks in advanced economies often require all banks to adhere to stringent cybersecurity standards. Analysis by [68] confirms that the first generation of cyber regulations were issued mainly in advanced economies (focusing on establishing a cyber risk management approach and controls), while over the last few years, authorities in emerging countries are either deficient in terms of cyber regulation or gradually followed suit and issued new/additional cyber regulations. This is additionally visible in average cybersecurity preparedness indices being higher in Europe and lower in Latin America, Africa and Asia [53].

In advanced economies, cyberattacks are associated with higher ROE, NIM and TCR, as these variables exhibit consistently positive and statistically significant coefficients across model specifications. Banks with higher NIM are more profitable and prominent. Such banks are more likely to attract wider media attention, publicizing their profitability and annual results, thus making them more recognizable for hackers as potential victims. Attacking these institutions can draw significant media attention to the perpetrators. Hackers may target such banks as symbols of economic inequality or corporate greed. By disrupting their operations, hackers aim to protest against perceived injustices in the financial system, while by handling larger volumes of transactions and managing vast sums of money, profitable banks become more lucrative targets for hackers. These results are close to those by [29], who, on a corporate sample, confirmed that more profitable firms are more prone to a cyberattack.

Criminals vs hacktivists

Next, we proceeded to assess the results modeled on the sample of attacks made by criminals and hacktivists separately, as two-thirds of the attacks (66%) were perpetrated by criminals, and one third (30%) by hacktivists (the rest remains undetermined). The detailed estimated results for these groups of countries are in the Appendix.

As illustrated in Figure 3, it turned out that the results for criminals are mostly in line with the conclusions on the basis of the full sample, underlying the importance of bank size, i.e., its total assets and deposit base (ln_TA and ln_DEP) from the criminals' perspective. These two variables have statistically significant coefficients, similar to those in the baseline model, but without the positive effect of TCR. At the same time, the coefficient for LIQ is negative and significant, but not consistent among all model specifications.

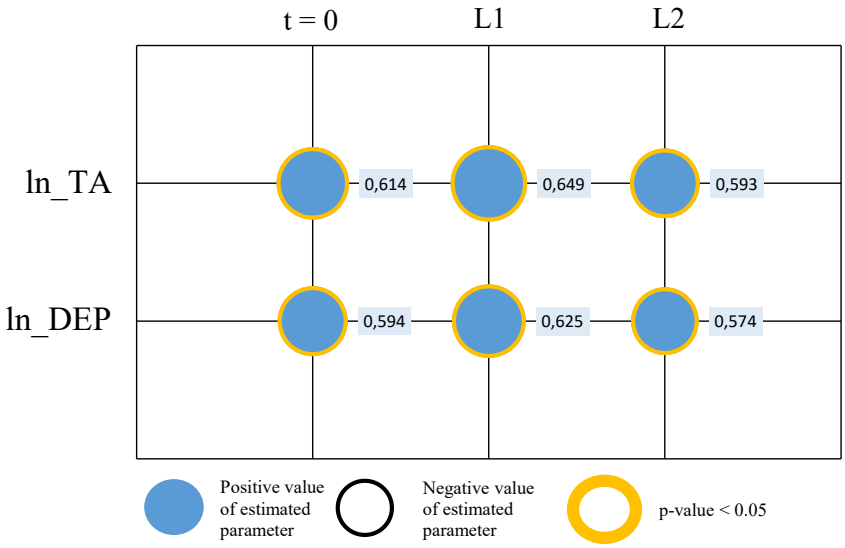
Surprisingly, the results for attacks by hacktivists didn't reveal the existence of any persistent conclusions regarding the statistically significant variables, confirming that their attacks are driven by non-monetary motives. When selecting their victims, hacktivists first of all choose a country, whose politics are not in line with their agenda, while the choice of attacked banks in this country might simply be a more or less random derivative thereof.

4.3. Robustness

In this section we estimate models from database B to act as robustness check of the results achieved in database A. In particular, the robustness of our results is achieved through:

- use of different, alternative profitability, resilience and liquidity measures - as described in the results in the previous section from panel models in database A;
- different estimation techniques - comparing estimations of panel modeling (in database A) with results of logistic regression (in database B);
- use of different samples – database A, containing data only on banks victimized by the cyberattack, and database B, containing data on banks attacked in 2023 (targets) and those not attacked (non-targets)[7];
- additionally conducting regressions using lagged values of the independent variables.

The results for a logistic regression in database B (for *t*=2023 and for models with lags of all the implemented independent variables) confirm the findings from the previous section and panel modeling, as ln_TA and ln_DEP are statistically significant with positive sign across all model specifications. The positive coefficients for TCR and NIM are not consistently significant across all model specifications, and the coefficients for other independent variables are insignificant. Figure 4 presents the magnitude of the estimated coefficients and their significance in the 2023 models (t=0), as well as in models with lagged independent variables (L1 and L2). The detailed estimated results are presented in the Appendix.



[7] Importantly, database B is based on publicly disclosed cyberattacks, and thus the absence of a recorded event should not be interpreted as the absence of an actual cyberattack.

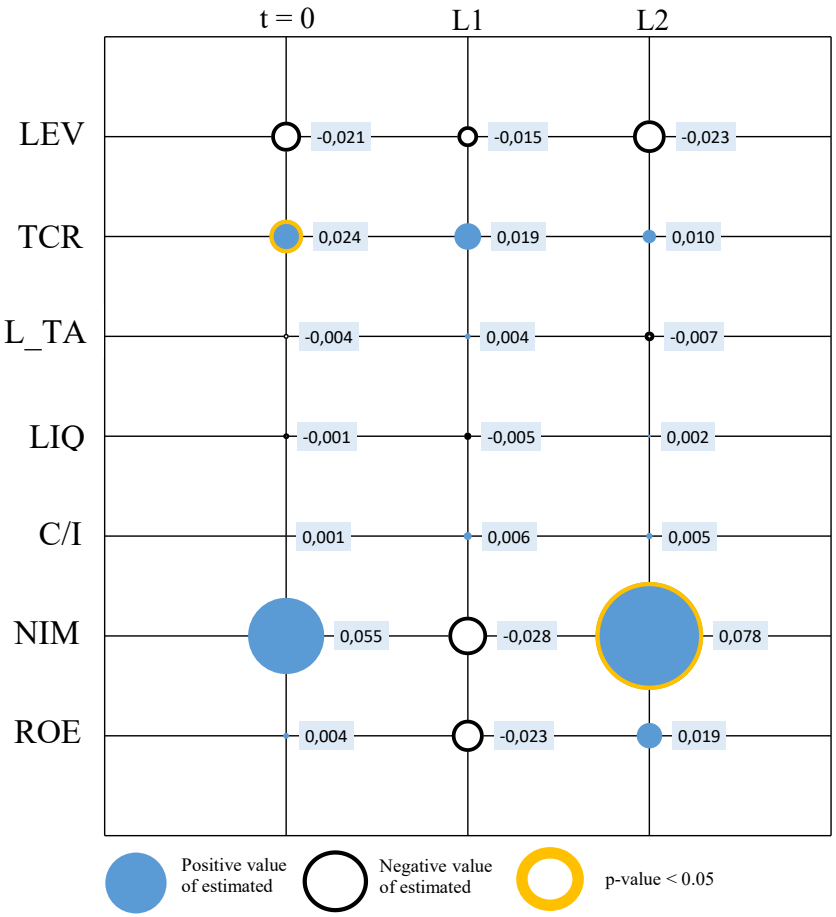


Figure 4 Estimated coefficients of bank-level financial variables and their significance using logistic regression on database B

Note: This figure presents the results of a logistic regression analysis where the dependent variable is the binary variable indicating the occurrence of a cyberattack in 2023 using database B. Each column represents separate estimation results depending on temporal observation of the independent variables: T=0 denotes variable from 2023, L1 represents the variable level recorded in 2022, and L2 represents the variable level recorded in 2021. The size of the circles indicates the level of the estimated parameter.

Alt text: A chart showing estimated effects of variables on the likelihood of a cyberattack across three time periods (current year and two previous years). Blue (white) circles indicate positive (negative) effects, circle size reflects the magnitude of the effect.

5. Conclusions and policy implications

This paper aimed to identify the financial determinants of cyberattacks on banks, as observed in publicly disclosed data, by examining which aspects of bank's financial standing are linked to a higher likelihood of such events. On a world-wide sample of 319 cyberattacks, which occurred in 53 countries between 2014 and 2024, we reach one major conclusion. The increasing size of the bank itself (its total assets and its growing deposit base) is consistently associated with a higher likelihood of cyberattacks, which confirms our research hypothesis. Estimations indicate that a 100% increase in a bank's assets raises the probability of a cyberattack by approximately 3.8 percentage points.

The results are robust to different model specifications (with different variants of bank-level variables), estimation methods (including both the Conditional Mixed Process estimator and logistic regression), as well as composition of the bank sample. However, estimating the results on subsamples (split among several dimensions) revealed additional insights. For example, the determinants of cyberattacks for US

banks are unique, where being a smaller, less resilient and inefficient bank makes it more likely to experience a cyberattack. In turn, cyberattacks in advanced countries are in general driven by higher ROE, NIM and TCR.

The interpretation of results follows the lens of expected payoff for cyber attackers. Rational hackers select their targets to maximize expected payoff (benefits minus costs). This might result in their decision to attack both bigger banks (as we found the whole sample) but also smaller ones (as in the case of US banks). Hackers attack high-value targets such as large banks, where strong defenses increase attack costs, but potential rewards (monetary for criminals and publicity gains for hacktivists) are very substantial. As for smaller banks – they might be easier (cheaper) to compromise but yield smaller gains. Whichever option is optimal depends on the attacker's technical capabilities and objectives. Our results support such logic of a hacker's mindset, which applies both to financially motivated actors (cybercriminals) and to those seeking visibility or publicity (hacktivists).

However, the presented research is not without limitations. The main obstacle, as in many studies on cyber risk, is the scarcity of comprehensive and reliable data on cyber incidents and their subsequent economic and social ramifications. Enriching the analyzed data sample will likely lead to more robust results in the future. Many countries also lack harmonized rules regulating transparency and reporting obligations for cyberattacks on banks. Only recently, since the start of 2025, did the implementation of Digital Operational Resilience Act (Regulation (EU) 2022/2554) in the EU make financial entities obligated to submit reports on a major ICT-related incident or significant cyber threat to relevant national competent authorities. While these reports remain confidential and not publicly disclosed, it is a step in the right direction. That is why, at this stage, given the prevalent data gaps, the positive relationship between bank size may therefore partially reflect more strict cyber incident disclosure requirements for bigger banks, rather than determinants of targeting hackers.

Our results point to actionable policy implications for supervisors and banks. Policymakers should continue regulatory efforts to develop reporting requirements and enable more access to data on cyberattacks on financial institutions. As cyber risk is a growing threat to the stability of banks and no longer just an operational risk concern, it should be much higher on the agenda of both micro- and macroprudential supervisors. It is essential to recognize cybersecurity as not merely a technical IT issue, but as material risk with consequences for the health and profitability of the bank. For instance, supervisors within the Supervisory Review and Evaluation Process should pay more attention to cyber risk exposure, especially for bigger banks with a more significant deposit base – in line with our results. Indeed, [69] empirically prove that targeted supervisory scrutiny, implemented through a non-capital-based stress test by the ECB, can effectively discipline and motivate lagging banks to remedy under-investment in their cyber defenses, ultimately enhancing systemic stability in the face of growing cyber-related risks. As for banks themselves, apart from back-up procedures, they should continue to educate and increase awareness about cybersecurity among their staff, at all management levels, given that past cases clearly indicate hackers often using social engineering on bank employees to launch their cyberattacks. In particular, banks in the US can be advised to improve their efficiency and capital adequacy, as well as invest more in the resilience of IT infrastructure, to reduce the risk of experiencing a cyberattack. Our results indicate that it is crucial for banks to establish integrated risk management framework tailored for banking systems, designed to assess and manage cybersecurity risks associated with digital banking services [70].

Directions of future studies are numerous and could include studies on cyberattacks on other non-bank financial institutions like crypto currency exchanges or investment funds. Moreover, advancing work on potential measures of both cyber risk exposure on a bank level, as well as measures of cyber resilience, continue to remain challenging but worthy of scientific pursuits. Furthermore, the determinants of cyber runs and impact of cyberattacks on a bank customers' behavior, as well as their adoption of digital technologies are also open for further exploration. The study of how AI is used by hackers to augment

their attacks, and how it can be implemented to improve cyber resilience likewise remains at the urgent forefront of research needs [71].

Acknowledgements:

The opinions expressed herein are those of the authors and do not reflect those of the associated institutions. Authors express gratitude to the anonymous Reviewers and the Editor for their very useful comments, which were helpful in improving the quality of this research paper.

References

1. Vergara Cobos E. Cybersecurity Economics for Emerging Markets. World Bank; 2024. http://hdl.handle.net/10986/42130.
2. International Monetary Fund. Chapter 3, Cyber Risk — A Growing Concern for Macrofinancial Stability. Global Financial Stability Report. April 2024.
3. European Banking Authority. Risk Assessment Report — December 2025. Paris; 2025.
4. McCaul E. Cyber risk - a supervisory perspective. SCION Day, ECB; 22 October 2024.
5. Bouveret A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Paper WP/18/143. 2018.
6. Aldasoro I, Gambacorta L, Giudici P *et al.* The drivers of cyber risk. *J Financ Stab* 2022;**60**:100989. https://doi.org/10.1016/j.jfs.2022.100989.
7. Brando D, Kotidis A, Kovner A *et al.* Implications of Cyber Risk for Financial Stability. FEDS Notes. Board of Governors of the Federal Reserve System; 2022.
8. Adedeji O. Cyberattack Trends in the Financial Sector: Assessing the Risks and Strategies for Resilient Defense. *IRE Journals*. 2023 May;**6**(11):936. IRE 1707045. ISSN 2456-8880.
9. Yassin A, Almaayah M. Cyber security risk assessment for determining threats and countermeasures for banking systems. *Int J Cybersecur Eng Innov* 2026;**2026**(1).
10. Roodman D. Fitting fully observed recursive mixed-process models with cmp. *Stata J* 2011;**11**(2):159–206.
11. Bencivelli L, Calabrese R, Lauridsen N. Understanding Cyber Risk: Drivers and Impacts on Firms. RSC Working Paper 2026/01. Robert Schuman Centre for Advanced Studies, Florence School of Banking and Finance, European University Institute; 2026.
12. Tsohou A, Diamantopoulou V, Gritzalis S et al. Cyber insurance: state of the art, trends and future directions. *Int J Inf Secur* 2023;**22**:737–748. https://doi.org/10.1007/s10207-023-00660-8.
13. Rangu CM, Badea L, Scheau MC *et al.* Cyber insurance risk analysis framework considerations. *J Risk Financ* 2024;**25**(2):224–252. https://doi.org/10.1108/JRF-10-2023-0245.
14. Smaga P. Evaluating cyber attacks on central banks — identification of trends in cyber threat landscape. *Comput Secur*. 2026;**160**:104742. https://doi.org/10.1016/j.cose.2025.104742.
15. Jin J, Li N, Liu S *et al.* Cyber attacks, discretionary loan loss provisions, and banks' earnings management. *Finance Res Lett* 2023;**54**:103705. https://doi.org/10.1016/j.frl.2023.103705.
16. Rahman MHF, Abdullah M, Sulong Z *et al.* Cybersecurity risk and bank competition. *J Int Financ Mark Inst Money* 2026;**109**:102313. https://doi.org/10.1016/j.intfin.2026.102313.
17. Baker SD, Ratnadiwakara D. Cyber Risk in Banking: Measuring and Predicting Vulnerability. Working paper. Federal Reserve Bank of Richmond; 2025.
18. Tajalizadehkhoob ST, Asghari H, Gañán C *et al.* Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware. In: Proceedings of the 13th Annual Workshop on the Economics of Information Security (WEIS); 2014.
19. Strupczewski G. Defining cyber risk. *Saf Sci* 2021;**135**:105143. https://doi.org/10.1016/j.ssci.2020.105143.
20. Woods DW, Böhme R. Systematization of Knowledge: Quantifying Cyber Risk. In: Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP); 2021 May 24–27; San Francisco, CA. p. 211–228. doi:10.1109/SP40001.2021.00053.
21. Wilson C, Gaidosch T, Adelmann F. *et al.* Cybersecurity Risk Supervision. Departmental Paper Series No. 19/15. IMF; 2019.
22. Curti F, Gerlach J, Kazinnik S. *et al.* Cyber risk definition and classification for financial risk management. *J Operational Risk* 2023;**18**(2). https://doi.org/10.21314/JOP.2022.036.
23. Shevchenko PV, Jang J, Malavasi M. *et al.* The nature of losses from cyber-related events: risk categories and business sectors. *J Cybersecur* 2023;**9**(1). https://doi.org/10.1093/cybsec/tyac016.
24. Aldasoro I, Gambacorta L, Giudici P, Leach T. Operational and cyber risks in the financial sector. *Int J Cent Bank* 2023;**19**(5):340–402.

25. Akinbowale OE, Klingelhöfer HE, Zerihun MF. Analytical hierarchy processes and Pareto analysis for mitigating cybercrime in the financial sector. *J Financ Crime* 2022;**29**(3):984–1008. https://doi.org/10.1108/JFC-04-2021-0086.
26. Pollmeier S, Bongiovanni I, Slapničar S. Designing a financial quantification model for cyber risk: A case study in a bank. *Saf Sci* 2023;**159**:106022. https://doi.org/10.1016/j.ssci.2022.106022.
27. Naveenan RV, Suresh G. Cyber risk and the cost of unpreparedness of financial institutions. In: Abedin MZ, Hajek P (ed). *Cyber Security and Business Intelligence: Innovations and Machine Learning for Cyber Risk Management*. Routledge; 2023.
28. Spanos G, Angelis L. The impact of information security events to the stock market: a systematic literature review. *Comput Secur* 2016;**58**:216–229. https://doi.org/10.1016/j.cose.2015.12.006.
29. Kamiya S, Kang JK, Kim J. *et al.* Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *J Financ Econ* 2021;**139**(3):719–749. https://doi.org/10.1016/j.jfineco.2019.05.019.
30. Tosun OK. Cyber-attacks and stock market activity. *Int Rev Financ Anal* 2021;**76**:101795. https://doi.org/10.1016/j.irfa.2021.101795.
31. Reserve Bank of New Zealand. Cyber incident cost estimates and the importance of building resilience. Reserve Bank of New Zealand Bulletin. 2020;84(2). February 2020.
32. Boungou W. Cyber-attacks and banking intermediation. *Econ Lett* 2023;**233**:111354. https://doi.org/10.1016/j.econlet.2023.111354.
33. Lending C, Minnick K, Schorno PJ. Corporate governance, social responsibility, and data breaches. *Financ Rev* 2018;**53**:413–455. https://doi.org/10.1111/fire.12160.
34. Duffie D, Younger J. Cyber Runs. Hutchins Center Working Paper Series No 51. Hutchins Center on Fiscal & Monetary Policy at Brookings; 2019.
35. Durongkadej I, Wang HE. Data breach announcement effect on bank loans, deposits, and stock performance. *J Financ Serv Res* 2025; **68**: 423–460. https://doi.org/10.1007/s10693-025-00447-z.
36. Koo H, van der Molen R, Vermeulen R, Verhoeks R, Pollastri A. A macroprudential perspective on cyber risk. Occasional Studies. 2022;20(1). DNB.
37. Heo Y. Cybersecurity and bank distance-to-default. Swiss Finance Institute Research Paper No. 25-69; 2023. https://doi.org/10.2139/ssrn.4660090.
38. Murphy A, Tindall ML, Klemme K *et al.* What Drives Cyber Losses at U.S. Banks? Potential Statistical Markers. Federal Reserve Bank of Dallas Working Paper 2520. Dallas (TX): Federal Reserve Bank of Dallas; 2025. doi:10.24149/wp2520.
39. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *J Cybersecur* 2019;**5**(1). https://doi.org/10.1093/cybsec/tyz013.
40. Bruno E, Pistolesi F, Teti E. Cybersecurity policy, ESG and operational risk: A virtuous relationship to improve banks' performance. *Int Rev Econ Finance* 2025;**99**:104053. https://doi.org/10.1016/j.iref.2025.104053.
41. European Systemic Risk Board. Systemic cyber risk. Frankfurt; 2020.
42. Welburn JW, Strong AM. Systemic cyber risk and aggregate impacts. *Risk Anal* 2022;**42**:1606–1622. https://doi.org/10.1111/risa.13715.
43. Poljšak B. Cyber mapping as a tool for monitoring cyber risk. Discussion Paper. Banka Slovenije; October 2024.
44. Bank of England. Financial Stability in Focus: The FPC's macroprudential approach to operational resilience. Financial Policy Committee. March 2024.
45. Eisenbach TM, Kovner A, Lee MJ. Cyber risk and the U.S. financial system: a pre-mortem analysis. *J Financ Econ* 2022;**145**(3):802–826. https://doi.org/10.1016/j.jfineco.2021.10.007.
46. Diamond DW, Dybvig PH. Bank runs, deposit insurance, and liquidity. *J Polit Econ* 1983;**91**(3):401–419.
47. Eisenbach TM, Kovner A, Lee MJ. When it rains, it pours: cyber vulnerability and financial conditions. *Econ Policy Rev* Federal Reserve Bank of New York. 2025;**31**(1):1–24.
48. Gaies B, Chaâbane N, Sahut J. Cyber risk, market fear and financial instability: hunting down risk through contagion analysis. Journal of Economic Studies. 2025;ahead-of-print. https://doi.org/10.1108/JES-02-2025-0131.
49. Kryshtal H, Samofalova M, Sakhno L *et al.* Cyber risks in the financial and banking system: analysis of direct and systemic losses. Financial and Credit Activity: Problems of Theory and Practice. 2025;2(61):125–140. https://doi.org/10.55643/fcaptp.2.61.2025.4672.
50. Vermeulen R, Sydow M, Brousse C. *et al.* Cyber resilience stress testing from a macroprudential perspective. Macroprudential Bulletin. ECB; March 2025.
51. Khiaonarong T, Korpinen KN, Islam E. Using simulations for cyber stress testing exercises. IMF Working Paper WP/25/85; 2025. https://doi.org/10.5089/9798229008952.001.
52. European Systemic Risk Board. Mitigating systemic cyber risk. Frankfurt; 2022.

53. Ravikumar R. Strengthening Cybersecurity: Lessons from the Cybersecurity Survey. Technical Notes and Manuals No. TNM/2025/06. IMF; 2025. https://doi.org/10.5089/9798400296864.005.
54. Abukari K, Dutta S, Li C. *et al.* Corporate communication and likelihood of data breaches. *Int Rev Econ Finance* 2024;**94**:103433. https://doi.org/10.1016/j.iref.2024.103433.
55. Florackis C, Louca C, Michaely R. *et al.* Cybersecurity risk. *Rev Financ Stud* 2023;**36**(1):351–407. https://doi.org/10.1093/rfs/hhac024.
56. Jamilov R, Rey H, Tahoun A. The anatomy of cyber risk. Institute for New Economic Thinking Working Paper Series No. 206; 2023. Available at SSRN: https://ssrn.com/abstract=4470871.
57. Cremer F, Sheehan B, Fortmann M. *et al.* Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues Pract* 2022;**47**:698–736. https://doi.org/10.1057/s41288-022-00266-6.
58. Harry C, Gallagher N. Classifying cyber events: a proposed taxonomy. *J Inf Warfare* 2018;**17**(3).
59. Harry C, Gallagher N. Categorizing cyber effects. In: Carayannis E, Grigoroudis E, Campbell DFJ, Katsikas SK (ed). *The Elgar Companion to Digital Transformation, Artificial Intelligence and Innovation in the Economy, Society and Democracy*. Edward Elgar Publishing; 2023.
60. Smaga P. Profiling the victim — cyber risk in commercial banks. *Comput Secur* 2025;**150**:104274. https://doi.org/10.1016/j.cose.2024.104274.
61. Uddin MH, Mollah S, Islam N. *et al.* Does digital transformation matter for operational risk exposure? *Technol Forecast Soc Change* 2023;**197**:122919. https://doi.org/10.1016/j.techfore.2023.122919.
62. Uddin MH, Ali MH, Hassan MK. Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Manag* 2020;**22**:239–309. https://doi.org/10.1057/s41283-020-00063-2.
63. Gogolin F, Lim I, Vallascas F. Cyberattacks on small banks and the impact on local banking markets. *J Money Credit Bank* 2026. Advance online publication. https://doi.org/10.1111/jmcb.70043.
64. Arellano M, Bond S. Some tests of specification for panel data: Monte Carlo evidence and an application to employment equations. *Rev Econ Stud* 1991;**58**(2):277–297. https://doi.org/10.2307/2297968.
65. Blundell R, Bond S. Initial conditions and moment restrictions in dynamic panel data models. *J Econometrics* 1998;**87**(1):115–143. https://doi.org/10.1016/S0304-4076(98)00009-8.
66. Edwards J, Coutts I, McLeod S. *et al.* Handling legacy IT in banking by using object design patterns to separate business and IT issues. In: Henderson P, (ed). *Systems Engineering for Business Process Change*. Springer; 2000. https://doi.org/10.1007/978-1-4471-0457-5.
67. Hayretci HE, Aydemir FB. A multi case study on legacy system migration in the banking industry. In: La Rosa M, Sadiq S, Teniente E (ed). *Advanced Information Systems Engineering — CAiSE 2021*. Lecture Notes in Computer Science, Vol. 12751. Springer, Cham; 2021. https://doi.org/10.1007/978-3-030-79382-1_32.
68. Crisanto JC, Pelegrini JU, Prenio J. Banks' cyber security – a second generation of regulatory approaches. FSI Insights on policy implementation No 50. BIS; 2023.
69. Abidi N, Gambacorta L, Kok C *et al.* Disciplining Digital Risk: Evidence from Cyber Stress Tests. Preliminary draft 29 Aug 2025, Federal Reserve Bank of Boston; 2025.
70. Azura YTY, Azad MA, Ahmed Y. An integrated cyber security risk management framework for online banking systems. *J Bank Financ Technol*. 2025;**9**:85–104. doi:10.1007/s42786-025-00056-3.
71. Crisanto JC, Leuterio CB, Prenio J. *et al.* Regulating AI in the financial sector: recent developments and main challenges. FSI Insights on policy implementation No 63. BIS; 2024.

Annex

Table A1. Descriptive statistics (database B)

Variable	Obs	Mean	Std. Dev.
ln_TA_t	12,056	12.3773	2.357759
ln_DEP_t	11,749	11.99288	2.352227
ROE_t	11,983	8.250367	9.012856
NIM_t	12,012	4.170289	3.253514
C_I_t	12,007	74.76035	21.81
TCR_t	4,812	19.71541	10.31936
LEV_t	12,047	13.17075	11.72288
L_TA_t	11,989	59.92848	19.27392
LIQ_t	11,796	31.34827	25.45856
ln_GDPpc_t	12,824	11.00859	0.7509506
CPI_t	12,824	4.359444	1.202831

Variable	Obs	Mean	Std. Dev.
ln_TA_L1	12,337	12.30325	2.344831
ln_DEP_L1	12,021	11.96076	2.32908
ROE_L1	12,280	6.699599	8.591447
NIM_L1	12,294	3.778994	3.003425
C_I_L1	12,295	77.31462	23.39292
TCR_L1	4,975	19.45771	10.57952
LEV_L1	12,329	12.46035	11.70868
L_TA_L1	12,266	57.93745	19.51683
LIQ_L1	12,079	32.65995	25.71057
ln_GDPpc_L1	12,824	10.94475	0.7580547
CPI_L1	12,824	8.091519	1.106026

Variable	Obs	Mean	Std. Dev.
ln_TA_L2	12,665	12.23441	2.35107
ln_DEP_L2	12,356	11.89717	2.343698
ROE_L2	12,612	6.022284	8.511611
NIM_L2	12,626	3.537521	2.791137
C_I_L2	12,622	79.98781	25.16822
TCR_L2	5,046	19.80158	10.55653
LEV_L2	12,662	13.15492	11.23291
L_TA_L2	12,600	53.67905	18.42532
LIQ_L2	12,405	38.02701	24.0753
ln_GDPpc_L2	12,824	10.86203	0.7614392
CPI_L2	12,824	4.782196	1.406835

Note: L indicates the number of the lag

Source: own work

Table A2. Results for US banks (database A)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	-0.1255**	-0.1170***	-0.1277**	-0.1162***	-0.1227**	-0.1137***	-0.1262**	0.0248**	-0.1199**	-0.1045***	-0.1202**	-0.1039***
	(0.0438)	(0.0228)	(0.0416)	(0.0192)	(0.0449)	(0.0228)	(0.0424)	(0.0089)	(0.0439)	(0.0230)	(0.0416)	(0.0195)
Profitability measure (estimations)	-0.0021	-0.0024*	-0.0019	-0.0026*	0.0066	0.0199	0.0107	0.0044	0.0025	0.0019**	0.0024	0.0018**
	(0.0024)	(0.0011)	(0.0024)	(0.0011)	(0.0281)	(0.0139)	(0.0289)	(0.0045)	(0.0013)	(0.0006)	(0.0013)	(0.0006)
Resilience measure (estimations)	-0.0084	-0.0085**	-0.0087	-0.0122***	-0.0084	-0.0109***	-0.0088	-0.0030	-0.0078	-0.0093**	-0.0080	-0.0121***
	(0.0045)	(0.0030)	(0.0045)	(0.0031)	(0.0045)	(0.0031)	(0.0045)	(0.0018)	(0.0045)	(0.0030)	(0.0045)	(0.0031)
Liquidity measure (estimations)	0.0005	-0.0010	0.0002	0.0001	-0.0008	0.0007	-0.0001	-0.0005	0.0006	0.0006	-0.0007	0.0001
	(0.0018)	(0.0009)	(0.0018)	(0.0006)	(0.0016)	(0.0006)	(0.0020)	(0.0006)	(0.0018)	(0.0006)	(0.0015)	(0.0006)
CPI	-0.0482***	-0.0133**	-0.0481***	-0.0139**	-0.0495***	-0.0129**	-0.0494***	0.0045***	-0.0465***	-0.0127**	-0.0464***	-0.0136**
	(0.0085)	(0.0047)	(0.0085)	(0.0046)	(0.0084)	(0.0046)	(0.0085)	(0.0010)	(0.0085)	(0.0046)	(0.0085)	(0.0046)
ln_GDPpc	2.0089***	1.0771***	2.0277***	1.1037***	2.0095***	1.0751***	2.0332***	0.2989***	1.9823***	1.0371***	1.9977***	1.0541***
	(0.1803)	(0.0822)	(0.1799)	(0.0796)	(0.1804)	(0.0833)	(0.1799)	(0.0310)	(0.1805)	(0.0826)	(0.1801)	(0.0790)
Fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	611	1317	611	1317	611	1317	611	3552	611	1317	611	1317

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001

Table A3. Results for non-US banks (database A)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.0727***	0.0686***	0.0475***	0.0343**	0.0729***	0.0711***	0.0465***	0.0355***	0.0655***	0.0631***	0.0420***	0.0314**
	(0.0178)	(0.0172)	(0.0123)	(0.0106)	(0.0177)	(0.0168)	(0.0121)	(0.0104)	(0.0181)	(0.0174)	(0.0125)	(0.0106)
Profitability measure (estimations)	-0.0003	0.0003	-0.0004	0.0004	0.0066	0.0078	0.0045	0.0068	-0.0006	-0.0008	-0.0006	-0.0009*
	(0.0006)	(0.0006)	(0.0007)	(0.0006)	(0.0054)	(0.0049)	(0.0055)	(0.0050)	(0.0005)	(0.0004)	(0.0005)	(0.0004)
Resilience measure (estimations)	0.0033**	-0.0000	0.0034**	-0.0003	0.0035**	-0.0005	0.0031**	-0.0012	0.0031**	-0.0004	0.0036**	-0.0009
	(0.0012)	(0.0022)	(0.0012)	(0.0022)	(0.0012)	(0.0022)	(0.0012)	(0.0022)	(0.0011)	(0.0022)	(0.0012)	(0.0022)
Liquidity measure (estimations)	-0.0006	-0.0010	-0.0006	-0.0003	-0.0006	-0.0004	-0.0005	-0.0009	-0.0007	-0.0004	-0.0005	-0.0003
	(0.0008)	(0.0007)	(0.0008)	(0.0005)	(0.0005)	(0.0005)	(0.0008)	(0.0007)	(0.0008)	(0.0005)	(0.0005)	(0.0005)
CPI	0.0030*	0.0035**	0.0029*	0.0033**	0.0027*	0.0031**	0.0029*	0.0033**	0.0028*	0.0030**	0.0026*	0.0030**
	(0.0012)	(0.0011)	(0.0012)	(0.0011)	(0.0012)	(0.0011)	(0.0012)	(0.0011)	(0.0012)	(0.0011)	(0.0012)	(0.0011)
ln_GDPpc	0.1127**	0.1206**	0.1411***	0.1637***	0.1022*	0.1096**	0.1339***	0.1461***	0.1142**	0.1236**	0.1402***	0.1591***
	(0.0420)	(0.0402)	(0.0396)	(0.0372)	(0.0425)	(0.0402)	(0.0399)	(0.0375)	(0.0419)	(0.0399)	(0.0394)	(0.0369)
Fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	2086	2221	2086	2217	2078	2231	2089	2235	2088	2230	2077	2230

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001

Table A4. Results for banks in advanced countries (database A)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.0072	-0.0269	0.0136	-0.0156	0.0164	-0.0267	0.0229	-0.0099	0.0143	-0.0251	0.0206	-0.0129
	(0.0240)	(0.0180)	(0.0213)	(0.0122)	(0.0238)	(0.0179)	(0.0209)	(0.0120)	(0.0244)	(0.0184)	(0.0217)	(0.0123)
Profitability measure (estimations)	0.0028*	0.0016*	0.0027*	0.0016*	0.0370*	0.0182*	0.0396**	0.0190*	-0.0002	0.0000	-0.0001	0.0001
	(0.0011)	(0.0008)	(0.0011)	(0.0008)	(0.0146)	(0.0079)	(0.0144)	(0.0079)	(0.0006)	(0.0005)	(0.0007)	(0.0005)
Resilience measure (estimations)	0.0047**	-0.0031	0.0047**	-0.0029	0.0056**	-0.0035	0.0050**	-0.0033	0.0050**	-0.0024	0.0055**	-0.0024
	(0.0016)	(0.0026)	(0.0016)	(0.0027)	(0.0018)	(0.0027)	(0.0016)	(0.0027)	(0.0016)	(0.0026)	(0.0018)	(0.0027)
Liquidity measure (estimations)	0.0006	-0.0002	0.0006	-0.0005	-0.0004	-0.0002	-0.0001	-0.0005	0.0007	-0.0004	-0.0009	-0.0005
	(0.0011)	(0.0008)	(0.0011)	(0.0005)	(0.0008)	(0.0005)	(0.0012)	(0.0008)	(0.0011)	(0.0005)	(0.0008)	(0.0005)
CPI	0.0007	0.0039	0.0007	0.0033	0.0007	0.0031	0.0015	0.0036	0.0017	0.0037	0.0007	0.0037
	(0.0041)	(0.0031)	(0.0041)	(0.0031)	(0.0041)	(0.0031)	(0.0040)	(0.0031)	(0.0041)	(0.0031)	(0.0041)	(0.0031)
ln_GDPpc	0.6419***	0.6396***	0.6312***	0.6121***	0.6317***	0.6558***	0.6120***	0.6261***	0.6419***	0.6402***	0.6317***	0.6161***
	(0.0889)	(0.0612)	(0.0878)	(0.0558)	(0.0887)	(0.0619)	(0.0878)	(0.0557)	(0.0893)	(0.0621)	(0.0883)	(0.0559)
Fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	1575	2321	1575	2310	1564	2310	1575	2321	1575	2310	1564	2310

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001

Table A5. Results for banks in emerging and developing economies (database A)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.0749**	0.0679**	0.0417**	0.0410**	0.0731**	0.0707***	0.0358*	0.0366**	0.0691**	0.0663**	0.0357*	0.0363*
	(0.0232)	(0.0213)	(0.0146)	(0.0141)	(0.0234)	(0.0209)	(0.0145)	(0.0141)	(0.0236)	(0.0213)	(0.0148)	(0.0142)
Profitability measure (estimations)	-0.0021**	-0.0012	-0.0022**	-0.0010	0.0036	0.0064	0.0004	0.0046	-0.0001	-0.0002	-0.0001	-0.0003
	(0.0008)	(0.0007)	(0.0008)	(0.0007)	(0.0060)	(0.0058)	(0.0060)	(0.0059)	(0.0006)	(0.0006)	(0.0006)	(0.0006)
Resilience measure (estimations)	0.0001	-0.0026	0.0000	-0.0027	0.0001	-0.0039	-0.0005	-0.0041	-0.0003	-0.0034	0.0000	-0.0037
	(0.0016)	(0.0025)	(0.0016)	(0.0025)	(0.0016)	(0.0025)	(0.0016)	(0.0025)	(0.0016)	(0.0024)	(0.0016)	(0.0025)
Liquidity measure (estimations)	-0.0014	-0.0015	-0.0015	0.0002	0.0000	-0.0000	-0.0013	-0.0011	-0.0013	0.0001	0.0001	0.0001
	(0.0009)	(0.0008)	(0.0009)	(0.0006)	(0.0007)	(0.0006)	(0.0009)	(0.0008)	(0.0009)	(0.0006)	(0.0007)	(0.0006)
CPI	0.0014	0.0017	0.0013	0.0017	0.0015	0.0015	0.0014	0.0015	0.0015	0.0016	0.0014	0.0016
	(0.0013)	(0.0012)	(0.0013)	(0.0012)	(0.0013)	(0.0012)	(0.0013)	(0.0012)	(0.0013)	(0.0012)	(0.0013)	(0.0012)
ln_GDPpc	0.0692	0.0634	0.1041*	0.1012*	0.0575	0.0470	0.0950*	0.0776	0.0605	0.0585	0.1001*	0.0907*
	(0.0491)	(0.0467)	(0.0454)	(0.0435)	(0.0502)	(0.0471)	(0.0460)	(0.0440)	(0.0491)	(0.0463)	(0.0454)	(0.0432)
Fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	1122	1217	1122	1224	1125	1238	1125	1231	1124	1237	1124	1237

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001

Table A6. Results for banks attacked by criminals (database A)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.0434**	0.0357**	0.0298**	0.0179*	0.0426**	0.0360**	0.0289**	0.0187*	0.0431**	0.0399***	0.0292**	0.0198**
	(0.0135)	(0.0113)	(0.0097)	(0.0076)	(0.0135)	(0.0111)	(0.0096)	(0.0075)	(0.0137)	(0.0114)	(0.0098)	(0.0076)
Profitability measure (estimations)	-0.0002	-0.0001	-0.0003	0.0000	0.0007	-0.0005	0.0000	-0.0003	0.0001	0.0005	0.0001	0.0004
	(0.0005)	(0.0004)	(0.0005)	(0.0004)	(0.0044)	(0.0037)	(0.0044)	(0.0038)	(0.0004)	(0.0003)	(0.0004)	(0.0003)
Resilience measure (estimations)	0.0015	-0.0026	0.0016	-0.0024	0.0016	-0.0022	0.0015	-0.0028	0.0015	-0.0020	0.0017	-0.0022
	(0.0009)	(0.0015)	(0.0009)	(0.0015)	(0.0010)	(0.0015)	(0.0009)	(0.0015)	(0.0009)	(0.0015)	(0.0010)	(0.0015)
Liquidity measure (estimations)	0.0002	0.0003	0.0002	-0.0007*	-0.0005	-0.0007*	0.0002	0.0002	0.0002	-0.0007*	-0.0005	-0.0007*
	(0.0006)	(0.0005)	(0.0006)	(0.0003)	(0.0004)	(0.0003)	(0.0006)	(0.0005)	(0.0006)	(0.0003)	(0.0004)	(0.0003)
CPI	0.0012	0.0024**	0.0012	0.0024**	0.0011	0.0023**	0.0012	0.0025**	0.0012	0.0024**	0.0012	0.0025**
	(0.0009)	(0.0008)	(0.0009)	(0.0009)	(0.0009)	(0.0009)	(0.0009)	(0.0008)	(0.0009)	(0.0009)	(0.0009)	(0.0009)
ln_GDPpc	0.0665*	0.1509***	0.0835**	0.1720***	0.0641	0.1452***	0.0824**	0.1735***	0.0654*	0.1405***	0.0814**	0.1696***
	(0.0332)	(0.0289)	(0.0310)	(0.0262)	(0.0336)	(0.0288)	(0.0312)	(0.0262)	(0.0331)	(0.0288)	(0.0310)	(0.0260)
Fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	2697	3538	2697	3534	2689	3548	2700	3552	2699	3547	2688	3547

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001

Table A7. Results for banks attacked by hacktivists (database A)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.0202*	0.0039	0.0153*	0.0042	0.0204*	0.0042	0.0141*	0.0049	0.0174	0.0007	0.0132	0.0030
	(0.0093)	(0.0070)	(0.0067)	(0.0047)	(0.0092)	(0.0069)	(0.0066)	(0.0047)	(0.0094)	(0.0071)	(0.0067)	(0.0047)
Profitability measure (estimations)	-0.0005	-0.0001	-0.0005	-0.0001	0.0034	0.0052*	0.0027	0.0047*	-0.0002	-0.0003	-0.0002	-0.0003
	(0.0004)	(0.0003)	(0.0004)	(0.0003)	(0.0030)	(0.0023)	(0.0030)	(0.0024)	(0.0003)	(0.0002)	(0.0003)	(0.0002)
Resilience measure (estimations)	0.0011	0.0002	0.0011	0.0001	0.0010	-0.0006	0.0009	-0.0002	0.0010	-0.0004	0.0011	-0.0002
	(0.0006)	(0.0009)	(0.0006)	(0.0009)	(0.0007)	(0.0009)	(0.0006)	(0.0010)	(0.0006)	(0.0009)	(0.0007)	(0.0009)
Liquidity measure (estimations)	-0.0006	-0.0009**	-0.0006	0.0003	-0.0001	0.0002	-0.0005	-0.0008**	-0.0006	0.0003	-0.0001	0.0003
	(0.0004)	(0.0003)	(0.0004)	(0.0002)	(0.0003)	(0.0002)	(0.0004)	(0.0003)	(0.0004)	(0.0002)	(0.0003)	(0.0002)
CPI	0.0027***	0.0023***	0.0027***	0.0022***	0.0026***	0.0021***	0.0027***	0.0022***	0.0027***	0.0021***	0.0026***	0.0021***
	(0.0006)	(0.0005)	(0.0006)	(0.0005)	(0.0006)	(0.0005)	(0.0006)	(0.0005)	(0.0006)	(0.0005)	(0.0006)	(0.0005)
ln_GDPpc	0.1413***	0.1254***	0.1475***	0.1263***	0.1359***	0.1188***	0.1425***	0.1163***	0.1399***	0.1260***	0.1469***	0.1226***
	(0.0229)	(0.0180)	(0.0214)	(0.0162)	(0.0230)	(0.0179)	(0.0215)	(0.0164)	(0.0228)	(0.0179)	(0.0212)	(0.0162)
Fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	2697	3538	2697	3534	2689	3548	2700	3552	2699	3547	2688	3547

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001

Table A8. Results for banks attacked only in 2023 (database B) – no lag

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.567***	0.603***	0.602***	0.617***	0.596***	0.619***	0.609***	0.618***	0.560***	0.618***	0.607***	0.632***
	(0.0490)	(0.0341)	(0.0513)	(0.0355)	(0.0481)	(0.0363)	(0.0503)	(0.0359)	(0.0471)	(0.0372)	(0.0475)	(0.0366)
Profitability measure (estimations)	0.014	-0.000	0.011	-0.008	0.057	0.056	0.055	0.053	-0.004	0.003	-0.003	0.006
	(0.0151)	(0.0139)	(0.0151)	(0.0143)	(0.0317)	(0.0331)	(0.0334)	(0.0355)	(0.0091)	(0.0069)	(0.0094)	(0.0072)
Resilience measure (estimations)	0.019	0.005	0.027*	-0.025	0.027*	-0.035	0.026*	-0.032	0.017	-0.024	0.029*	-0.017
	(0.0124)	(0.0219)	(0.0130)	(0.0284)	(0.0133)	(0.0261)	(0.0131)	(0.0303)	(0.0122)	(0.0210)	(0.0133)	(0.0269)
Liquidity measure (estimations)	-0.002	-0.004	-0.003	0.002	-0.004	-0.002	-0.004	-0.005	-0.003	-0.002	0.000	0.002
	(0.0068)	(0.0053)	(0.0074)	(0.0042)	(0.0047)	(0.0039)	(0.0071)	(0.0057)	(0.0065)	(0.0038)	(0.0049)	(0.0042)
CPI	0.092*	0.111**	0.092*	0.110**	0.109**	0.112**	0.100**	0.101**	0.100**	0.111**	0.103**	0.108**
	(0.0391)	(0.0355)	(0.0392)	(0.0361)	(0.0398)	(0.0360)	(0.0381)	(0.0354)	(0.0378)	(0.0360)	(0.0391)	(0.0358)
ln_GDPpc	0.038	0.053	0.014	-0.024	0.083	0.056	0.039	0.029	0.040	0.007	0.015	-0.037
	(0.1116)	(0.1111)	(0.1096)	(0.1081)	(0.1132)	(0.1122)	(0.1104)	(0.1086)	(0.1119)	(0.1099)	(0.1130)	(0.1086)
N	4792	11928	4758	11673	4786	11767	4765	11721	4797	11756	4762	11697

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001

Table A9. Results for banks attacked only in 2023 (database B) – one-year lag

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.601***	0.649***	0.641***	0.669***	0.598***	0.642***	0.627***	0.646***	0.601***	0.659***	0.632***	0.677***
	(0.0450)	(0.0335)	(0.0479)	(0.0349)	(0.0448)	(0.0352)	(0.0475)	(0.0357)	(0.0454)	(0.0365)	(0.0465)	(0.0367)
Profitability measure (estimations)	-0.020	-0.023	-0.026	-0.032*	-0.035	-0.004	-0.052	-0.020	0.003	0.006	0.004	0.010
	(0.0158)	(0.0137)	(0.0159)	(0.0142)	(0.0477)	(0.0406)	(0.0535)	(0.0471)	(0.0075)	(0.0056)	(0.0079)	(0.0058)
Resilience measure (estimations)	0.014	0.007	0.026*	-0.022	0.018	-0.025	0.026*	-0.016	0.015	-0.022	0.024	-0.011
	(0.0104)	(0.0241)	(0.0106)	(0.0286)	(0.0119)	(0.0225)	(0.0111)	(0.0293)	(0.0100)	(0.0203)	(0.0125)	(0.0268)
Liquidity measure (estimations)	0.004	0.003	0.005	-0.003	-0.006	-0.007	0.005	0.004	0.004	-0.007	-0.003	-0.004
	(0.0062)	(0.0055)	(0.0067)	(0.0047)	(0.0047)	(0.0043)	(0.0067)	(0.0060)	(0.0062)	(0.0042)	(0.0050)	(0.0047)
CPI	0.249***	0.274***	0.243***	0.265***	0.252***	0.278***	0.250***	0.269***	0.251***	0.284***	0.239***	0.274***
	(0.0495)	(0.0463)	(0.0469)	(0.0458)	(0.0497)	(0.0463)	(0.0479)	(0.0447)	(0.0509)	(0.0484)	(0.0483)	(0.0469)
ln_GDPpc	0.078	0.097	0.040	0.036	0.082	0.089	0.015	0.026	0.068	0.074	0.037	0.022
	(0.1391)	(0.1365)	(0.1308)	(0.1254)	(0.1334)	(0.1308)	(0.1286)	(0.1238)	(0.1364)	(0.1313)	(0.1257)	(0.1255)
N	4958	12225	4923	11970	4947	12052	4925	11998	4959	12049	4925	11985

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001

Table A10. Results for banks attacked only in 2023 (database B) – two-year lag

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack
Bank size measure	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP	ln_TA	ln_TA	ln_DEP	ln_DEP
Profitability measure	ROE	ROE	ROE	ROE	NIM	NIM	NIM	NIM	C/I	C/I	C/I	C/I
Resilience measure	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV	TCR	LEV
Liquidity measure	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ	L_TA	L_TA	L_TA	LIQ	LIQ	LIQ
Bank size measure (estimations)	0.536***	0.585***	0.563***	0.600***	0.561***	0.601***	0.578***	0.606***	0.550***	0.611***	0.582***	0.627***
	(0.0440)	(0.0348)	(0.0453)	(0.0355)	(0.0435)	(0.0347)	(0.0452)	(0.0337)	(0.0456)	(0.0366)	(0.0440)	(0.0366)
Profitability measure (estimations)	0.031	0.010	0.030	0.003	0.054	0.096*	0.061	0.101*	0.001	0.006	0.003	0.008
	(0.0206)	(0.0183)	(0.0209)	(0.0197)	(0.0349)	(0.0396)	(0.0387)	(0.0410)	(0.0083)	(0.0060)	(0.0083)	(0.0061)
Resilience measure (estimations)	0.006	0.002	0.015	-0.024	0.007	-0.042	0.012	-0.040	0.006	-0.021	0.013	-0.015
	(0.0124)	(0.0209)	(0.0127)	(0.0267)	(0.0129)	(0.0268)	(0.0133)	(0.0305)	(0.0128)	(0.0187)	(0.0125)	(0.0247)
Liquidity measure (estimations)	-0.007	-0.004	-0.008	0.002	0.004	0.000	-0.009	-0.007	-0.006	-0.001	0.006	0.002
	(0.0068)	(0.0057)	(0.0072)	(0.0047)	(0.0047)	(0.0045)	(0.0079)	(0.0064)	(0.0072)	(0.0041)	(0.0047)	(0.0046)
CPI	-0.175	-0.085	-0.175	-0.068	-0.147	-0.099	-0.163	-0.111	-0.132	-0.062	-0.134	-0.066
	(0.1072)	(0.0940)	(0.1126)	(0.0995)	(0.0951)	(0.0964)	(0.1037)	(0.1017)	(0.0978)	(0.0896)	(0.1016)	(0.0934)
ln_GDPpc	-0.140	-0.143	-0.159	-0.197	-0.109	-0.125	-0.123	-0.147	-0.130	-0.182	-0.174	-0.224*
	(0.1112)	(0.1007)	(0.1126)	(0.1010)	(0.1114)	(0.1017)	(0.1117)	(0.0987)	(0.1146)	(0.1055)	(0.1193)	(0.1047)
N	5034	12562	5000	12305	5017	12383	5002	12337	5033	12379	4996	12318

Standard errors in parentheses; * p<0.05, **p<0.01, *** p<0.001