Chapter 3

CYBER RISK: A GROWING CONCERN FOR MACROFINANCIAL STABILITY

Online Annex 3.1 Data Description and Sources

Online Annex Table 3.1.1. Variable Description and Data Sources

Variable	Description	Source
Cyber-event-related variables		
Affected count	The total accumulated number of the identities breached or stolen, social security numbers revealed, devices compromised, etc. (depending on the loss type) across all resulting events	Advisen
Case type	Sub-grouping within a category describing more specifically the risk which resulted in the case	Advisen
Cyber incident	Binary value capturing whether a firm experienced a cyber incident in a year/quarter	Advisen; and IMF staff calculations
Cyber loss	Amount of a bank's loss in US dollars from cyber incidents in a given quarter	Advisen; and IMF staff calculations
Malicious cyber incident	Binary value capturing whether a firm experienced a malicious cyber incident in a year/quarter	Advisen; and IMF staff calculations
Total amount	The total accumulated cost associated with the ultimate parent organization linked to the incident. Where available, this total cost is broken down into its components in subsequent fields	Advisen
Firm-level Variables		
Age	Number of years since company's establishment. If establishment year is not available, number of years since incorporation	S&P Capital IQ
Asset intangibility	Intangible assets as a percentage of total assets	S&P Capital IQ
Capex ratio	Capital expenditure as a percentage of total assets	S&P Capital IQ
Cybersecurity policy	Binary variable that captures whether a company has a policy on cyber security in place to protect from cyberattack, unauthorized access, and data leaks	Refinitiv Datastream
Corporate governance score	ESG Corporate Governance Score	MSCI
Cybersecurity rating	Index ranging in value from 250 to 900, with the higher rating equaling better cybersecurity performance	Bitsight
Data privacy policy	Binary variable that captures whether a company has a policy to protect privacy and integrity of its customers and general public.	Refinitiv Datastream
Directors with cybersecurity experience	Number of members of the board of directors with cybersecurity experience, captured by the presence of cybersecurity related keywords in individual's biography	Orbis
Equity dividend yield	Annualized equity dividend yield, in percent, daily	Refinitive Datastream
Equity earning per share	Earning per share (EPS), daily	Refinitive Datastream
Equity market capitalization	Equity market capitalization, in local currency, daily	Refinitive Datastream
Equity prices	Equity price of individual stocks, in local currency, daily	Refinitive Datastream
Leverage	Total debt divided by total assets	S&P Capital IQ
Market capitalization	Market capitalization in US dollar	Orbis
Net income	Net Income, in millions of local currency	S&P Capital IQ
Operational income	Operational Income, in millions of local currency	S&P Capital IQ
Privacy and data security management score	Measures how well a company manages privacy and data security risks and opportunities. Higher scores indicate greater capacity to manage risk	MSCI
Privacy data management score	Management indicators measuring how well a company manages ESG risk and opportunities related to data privacy	MSCI
Retail deposit	Amount of domestic deposits (in transaction and nontransaction accounts) held by individuals in US dollars in a given quarter	Federal financial institutions Examination Council; and IMF staff calculations
Return on assets	Net income as a percentage of total assets	S&P Capital IQ
Revenue	Revenue, in millions of local currency	S&P Capital IQ
Teleworkability	Percentage of work force which can work remotely	Dingel and Nieman (2020)
Total assets	Total assets, in millions of local currency	S&P Capital IQ
Wholesale deposit	Amount of domestic deposits (in transaction and nontransaction accounts) held by non-depository institutions in US dollars in a given quarter	Federal financial institutions Examination Council; and IMF staff calculations
Country-level Variables		
Cyber legislation index	Index (ranging in value from 0 to 10) which assesses the adoption of e-commerce legislation in the fields of e-transactions, consumer protection, data protection/privacy and cybercrime	Verisk Maplecroft

Cyber risk index	Index (from 0 to 10) based on an assessment of legislation of consumer protection (e-commerce), cybercrime, data protection and privacy and e-transactions, as well as fixed (wired)-broadband subscriptions, percentage of made or received digital payments in the past year, research and development expenditure relative to GDP, and cyber threats from nation states	Verisk Maplecroft
Exchange rate	Exchange rate of local currency per US dollar	IMF
Geopolitical proximity	Foreign policy agreement based on countries' voting behavior in the UN General Assembly	Signorino and Ritter (1999); Häge (2011); IMF (2023)
Geopolitical risk index	Measure of adverse geopolitical events and associated risks based on a tally of newspaper articles covering geopolitical tensions	Caldara and Iacoviello (2022)
Global cybersecurity index	The global cybersecurity index measures the commitment of countries to cybersecurity at a global level, to raise awareness of the importance and different dimensions of the issue	International Telecommunication Union
Human capital index	Composite index adult literacy, gross enrolment ratio, expected years of schooling, mean years of schooling	UN E-Government Survey © 2022 by United Nations
International bandwidth	The international bandwidth mainly used to convey internet traffic and is the equivalent to international lines in the case of a public switch telephone network	International Telecommunication Union
Nominal gross domestic product	Nominal gross domestic product, in local currency and in US dollars	IMF
Short-term interest rate	Policy rate, daily	Haver, BIS
Stock market index	General stock market index, in local currency, daily	Refinitive Datastream
Telecommunications Infrastructure Index	Arithmetic average composite of five indicators: (i) estimated internet users per 100 inhabitants; (ii) number of main fixed telephone lines per 100 inhabitants; (iii) number of mobile subscribers per 100 inhabitants; (iv) number of wireless broadband subscriptions per 100 inhabitants; and (v) number of fixed broadband subscriptions per 100 inhabitants	United Nations

Source: IMF staff

Online Annex Table 3.1.2. List of Countries in the Sample

Advanced economies (AEs)	Emerging market and developing economies (EMDE)
Andorra, Australia, Austria, Belgium, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong SAR, Iceland, Ireland, Israel, Italy, Japan, Korea (the Republic of), Latvia, Lithuania, Luxembourg, Macao SAR, Malta, New Zealand, Norway, Portugal, Puerto Rico, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Taiwan Province of China, The Netherlands, United Kingdom, United States	Afghanistan, Albania, Algeria, Angola, , Argentina, Armenia, Aruba, Azerbaijan, Bahamas (The), Bahrain, Bangladesh, Barbados, Belarus, Belize, Bhutan, Bolivia, Bosnia and Herzegovina, Botswana, Brazil, Brunei Darussalam, Bulgaria, Cambodia, Cameroon, Chad, Chile, China, Colombia, Congo (Republic of), Costa Rica, Dominica, Dominican Republic, Ecuador, Egypt, El Salvador, Eswatini, Ethiopia, Fiji, , Gambia (The), Georgia, Ghana, Guatemala, Guyana, Haiti, Honduras, Hungary, India, Indonesia, Iran, Iraq, Jamaica, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyz Republic, Lao P.D.R., Lebanon, Lesotho, Liberia, Libya, Madagascar, Malawi, Malaysia, Maldives, Mali, Marshall Islands, Mauritania, Mauritius, Mexico, Moldova, Mongolia, Morocco, Mozambique, Myanmar, Namibia, Nauru, Nepal, Nicaragua, Nigeria, North Macedonia, Oman, Pakistan, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Poland, Qatar, Romania, Russia, Rwanda, Samoa, Saudi Arabia, Senegal, Serbia, Seychelles, Sierra Leone, Somalia, South Africa, Sri Lanka, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Sudan, Syria, Tajikistan, Thailand, Togo, Tonga, Trinidad and Tobago, Tunisia, Türkiye, Turkmenistan, Uganda, Ukraine, United Arab Emirates, Uruguay, Uzbekistan, Vanuatu, Venezuela, Vietnam, Yemen, Zambia, Zimbabwe

Note: Exact sample composition varies across empirical analyses based on data availability. The table uses International Organization for Standardization (ISO) country codes.

Classification of Financial Subsectors and Major Firms

Financial sector firms are classified into four subsectors (banks, insurers, asset managers, other financial firms) based on their 4-digit standard Industrial Classification (SIC) code.[1] Banks are classified as **'**G-

[1] Specifically, 'Banks' are defined as 'Commercial banks (6020)' 'National commercial banks (6021),' 'State commercial banks (6022),' 'Commercial banks, not elsewhere classified (6029),' 'Federal savings institutions (6035),' 'Savings institutions, except federal (6036),' 'Federal credit unions (6061),' 'State credit unions (6062),' 'Foreign banks and branches and agencies (6081),' 'Foreign trade and international banks (6082),' 'Bank holding companies (6712),' and 'Central reserve depository institutions, not elsewhere classified (6019).' 'Insurers' are defined as 'Life insurance (6311),' 'Accident and health insurance (6321),' 'Hospital and medical service plans (6324),' 'Fire, marine, and casualty insurance (6331),' 'Surety insurance (6351),' and 'Title insurance (6361).' 'Asset managers' are 'Investment advice (6282),' 'Management investment, open-ended (6722),' 'Investment offices, not elsewhere classified (6726),' and 'Miscellaneous business credit (6159).' 'Other financial' is defined as other categories whose 2-digit codes are 60-67 (except for 'Real estate (65)').

SIBs' based on the FSB's 2023 List of Global Systemically Important Banks (G-SIBs).[2] Major insurers are 25 firms ranked by 2021 net nonbanking assets.[3] Major asset managers are comprised of 30 firms ranked by their assets under management.[4] Top-20 FMIs are the 20 largest Payment Systems (PSs), Central Counterparties and Clearing Houses (CCPs) and Central Securities Depositories (CSDs) based on value of transactions (delivery instructions) in 2022 Redbook Statistics.[5]

Classification of Cyber Events

The complete list of case types identified by Advisen are: 'Cyber Extortion'; 'Data - Physically Lost or Stolen'; 'Data - Malicious Breach'; 'Data - Unintentional Disclosure'; 'Denial of Service (DDOS)/System Disruption'; 'Digital Breach/Identity Theft'; 'Identity - Fraudulent Use/Account Access'; 'Industrial Controls & Operations'; 'IT - Configuration/Implementation Errors'; 'IT - Processing Errors'; 'Network/Website Disruption'; 'Phishing, Spoofing, Social Engineering'; 'Privacy - Unauthorized Contact or Disclosure'; 'Privacy - Unauthorized Data Collection'; 'Skimming, Physical Tampering'; and 'Undetermined/Other'.

In this chapter, 'cyber incidents' are defined as all Advisen case types except for 'Privacy - Unauthorized Contact or Disclosure' and 'Privacy - Unauthorized Data Collection'.

'Malicious cyber incidents' or 'cyberattacks' are defined as 'Cyber Extortion', 'Data - Malicious Breach', 'Denial of Service (DDOS)/System Disruption'. 'Digital Breach/Identity Theft'; 'Undetermined/Other' 'Identity - Fraudulent Use/Account Access', 'Industrial Controls & Operations', 'Network/Website Disruption', 'Phishing, Spoofing, Social Engineering'; and 'Skimming, Physical Tampering.'

[2] See FSB (2023).

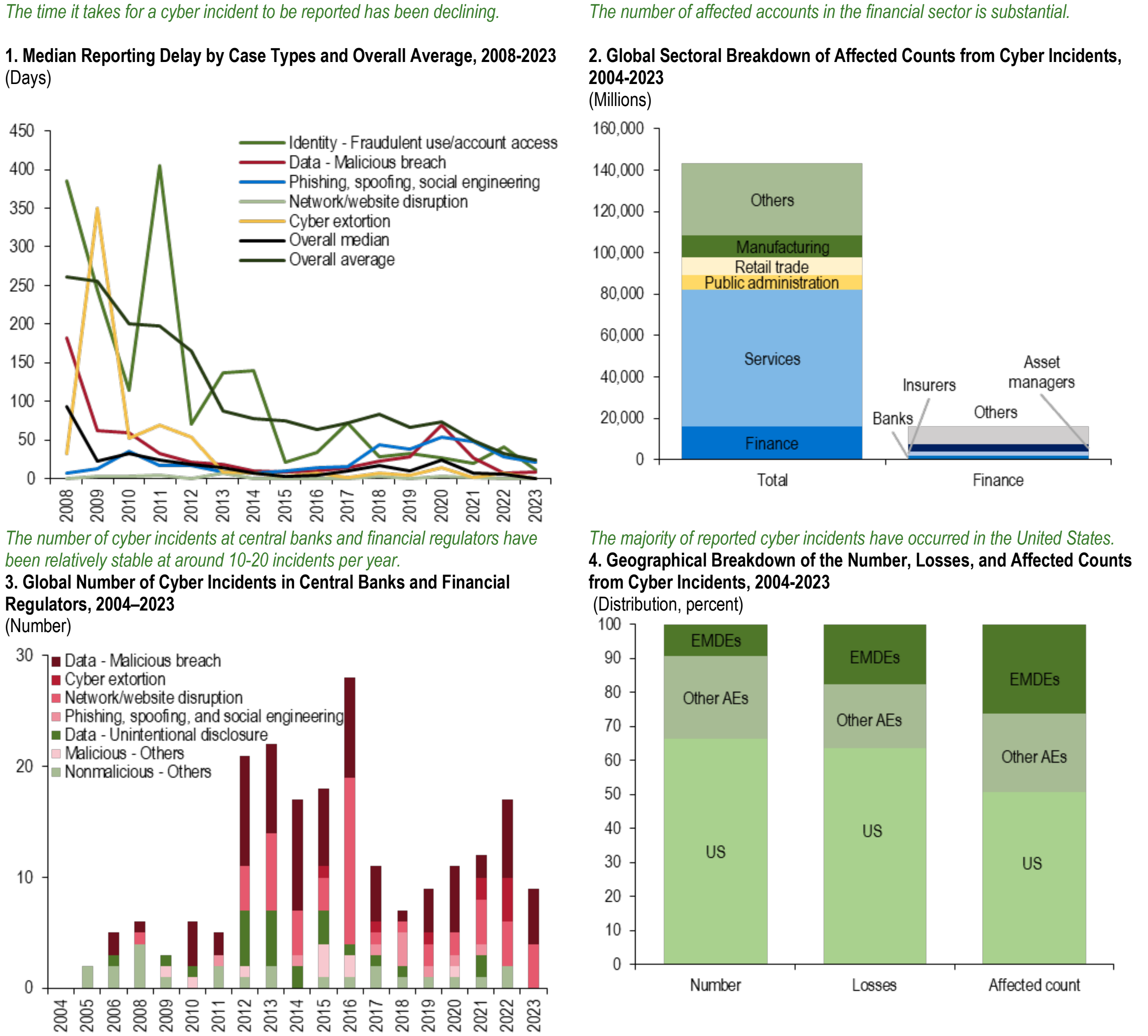
[3] See AM Best (2023).

[4] Asset managers included are the 20 largest firms by their assets under management according to P&I/Thinking Ahead Institute (2023), the 20 largest firms according to Sovereign Wealth Fund Institute (2023), and the 15 largest firms according to ADV (2023). In terms of asset managers, the selection process relies on multiple sources because the coverage of the managers in these rankings is different, depending on the definition of the asset managers by these institutions.

[5] See https://data.bis.org/topics/CPMI_FMI

Additional Stylized Facts

Online Annex Figure 3.1.1. Additional Stylized Facts on Cyber Incidents



The time it takes for a cyber incident to be reported has been declining.

1. Median Reporting Delay by Case Types and Overall Average, 2008-2023
(Days)

The number of affected accounts in the financial sector is substantial.

2. Global Sectoral Breakdown of Affected Counts from Cyber Incidents, 2004-2023
(Millions)

The number of cyber incidents at central banks and financial regulators have been relatively stable at around 10-20 incidents per year.

3. Global Number of Cyber Incidents in Central Banks and Financial Regulators, 2004–2023
(Number)

The majority of reported cyber incidents have occurred in the United States.

4. Geographical Breakdown of the Number, Losses, and Affected Counts from Cyber Incidents, 2004-2023
(Distribution, percent)

Sources: Advisen Cyber Loss Data; and IMF staff calculations.
Note: Panel 1 shows the time between a cyber incident occurring and its reporting. In panel 3, cyber incidents in central banks and financial regulations are identified by matching the names of central banks and regulators to those reported in the Advisen database. AEs = advanced economies; EMDEs = emerging market and developing economies.

Online Annex 3.2 Generalized Extreme Value Distribution of Cyber Loss

The Chapter analyzes cyber incident related extreme losses by approximating the distribution of maximum losses of a country within a year using a generalized extreme value (GEV) distribution. This annex explains the technical details of the analysis.

Model

The GEV distribution is defined as:

$$P\left(M_{Loss_c} \leq x\right) = \begin{cases} \exp\left(-\exp\left(-\left(\frac{x-\mu(X_c)}{\sigma(X_c)}\right)\right)\right), \ \xi = 0, \\ \exp\left(-\left(1+\xi\left(\frac{x-\mu(X_c)}{\sigma(X_c)}\right)\right)^{-\frac{1}{\xi}}\right), \ \xi \neq 0 \end{cases} \tag{1}$$

where $M_{Loss,c} = \widehat{M}_{Loss,c}/OI_c$, $\widehat{M}_{Loss_c}$ is the maximum loss in country *c* due to cyberattacks ($i = 1,2,\cdots I$) within a year ($= \max\{Loss_{i,c},\ i = 1,2,\cdots I\}$). Note that the distribution is constructed at the country level. To ensure the stationarity across countries, $\widehat{M}$ is scaled by the average operating income (OI_c) in country *c*. In addition, μ is a locational parameter, σ is a scale parameter, and ξ is a shape parameter. The following linear functions are assumed for the location and scale parameters, respectively.

$$\mu\left(X_{c,t}\right) = \beta_c + \beta \cdot X_{c,t}, \tag{2}$$

$$\sigma\left(X_{c,t}\right) = \exp\left(\gamma_c + \gamma \cdot X_{c,t}\right) \tag{3}$$

where β_c and γ_c are country fixed effects. The vector of control variables $X_{c,t} = (X_{c,k,t}, k = 1,2,\cdots,K)$ includes country size, penetration index of information and communication technology (ICT penetration), human capital, corporate governance, and geopolitical risks. $\beta = (\beta_k, k = 1,2,\cdots,K)$ and $\gamma = (\gamma_k, k = 1,2,\cdots,K)$ are the coefficients vectors to be estimated.

To study the implications of the higher/lower values of the location and shape parameters, the following quantile function is used:

$$Q(p;\mu(X_c),\sigma(X_c),\xi) = \mu(X_c) + \frac{\sigma(X_c)}{\xi}\left((-\log(p))^{-\xi} - 1\right) \text{ for } \xi \neq 0 \text{ and } 0 < p < 1 \tag{4}$$

where p is the percentile of the quantile function of interest that is increasing in $\mu(X_c)$ and also in $\sigma(X_c)$ if ξ is positive for $p > e^{-1} \simeq 0.368$.[1]

While equation (1) is a distribution function of the ratio of maximum losses to the average operating income in a country, the probability density function for the level of the maximum loss amount of a country can be obtained by transforming the variable and differentiating it with respect to the maximum loss. For any $z \in \mathbf{R}$, the density function of the maximum loss amount (in U.S. dollar) is then

$$f(z) = \begin{cases} \frac{1}{\sigma(X_c)\cdot OI_c}\exp\left(-(v(z)) - \exp\left(-v(z)\right)\right) & \text{if} \quad \xi = 0, z \in \mathbf{R}, \\ \frac{1}{\sigma(X_c)\cdot OI_c}\exp\left(-(1+\xi v(z))^{-\frac{1}{\xi}}\right)(1+\xi v(z))^{-\frac{1}{\xi}-1} & \text{if} \quad \xi \neq 0, \text{and } 1+\xi v(z) > 0 \end{cases} \tag{5}$$

where $v(z) = \frac{\frac{z}{OI_c} - \mu(X_c)}{\sigma(X_c)}$.

Bayesian Estimation

For each country *c*, the maximum loss of firms is computed as $\widehat{M}_{Loss_{c,t}} = \max\{Loss_{i,c,t},\ i = 1,2,\cdots I, t = 1,2,\cdots T\}$ where $Loss_{i,c,t}$ represents the sample i of country c's total amount of loss due to

[1] Note that when $\xi > 0$, p is very small ($p < e^{-1}$), μ is small, and σ is large, the quantile could take negative values.

a cyber incident in year t. To estimate equation (1), $M_{Loss,c,t}$ is obtained by scaling $\widehat{M}_{Lossc,t}$ by the average operating income of the country in each year. The average operating income is calculated using data from firms' profit and loss statements.[2]

Parametric assumptions of the model allow for the derivation of a conditional likelihood function for $M_{Loss_{c,t}}$. Based on the likelihood function and prior assumptions, estimation is carried out by the Markov-Chain Monte Carlo method with the Hamilton Monte Carlo algorithm. Estimation is carried out with 30,000 sample draws. The priors for the parameters are set as $(\beta_c, \beta_k, \gamma_c, \gamma_k, \xi) \sim N(0,10)$ for all $c \in \boldsymbol{C}$ and $k = 1,2,\cdots,K$, where $\boldsymbol{C}$ is the set of countries included in the sample, and K is the dimension of the control variables.[3] Given the uncertainty regarding the parameters, a sufficiently high variance parameter is chosen (compared to the posterior estimates).

Data

Losses due to cyber incidents are available for 13 countries from 2012 to 2022.[4] Countries with fewer than 10 observations per year are dropped from the sample leading to a total of 6,949 recorded losses. Control variables are:

- Country size (the percentage rank of a country's one year lagged nominal GDP in U.S. dollars over the full sample), as larger countries could be more likely to be exposed to cyber incidents.
- The degree of digitalization and digital literacy across countries (proxied by the United Nations' Telecommunication Infrastructure Index and Human Capital Index).
- Governance (Refinitiv governance scores), as firms with better governance could be better prepared for cyber incidents or less likely to be targeted by hackers.
- Geopolitical risk (country-level aggregate measure of similarity of foreign policies across country pairs based on their voting behavior in the United Nations General Assembly (UNGA) meetings).[5]

Results

Estimation results are summarized in Online Annex Table 3.2.1 and show that the size factor is strongly correlated with the location of extreme losses, while negatively correlated with the scale of extreme losses, indicating a non-linearity. Namely, the larger the country, the more it is exposed to cyber risk and the higher the losses on average, while extremely large losses seem to be somewhat contained perhaps because of better preparedness of major institutions or a greater capacity to respond. Consistent with this interpretation, a higher Telecommunication Infrastructure Index reduces the location of losses and also reduces the scale of the distribution of losses. Geopolitical proximity increases both the location and scale parameters. While this appears counterintuitive at first sight, countries that are geopolitically aligned to their investor countries are often advanced economies such as the U.S. and large European countries that are also often targeted by hackers. Baseline specification (6) in Online Annex Table 3.2.1 is reported in the main text, based on the AIC, BIC, and on the intuitiveness of the results.

[2] Note that average operating income is a country-level aggregate including all sectors. Direct matching of loss data and individual firms' balance sheet data is not feasible because too many firms with recorded losses cannot be matched. Alternative scaling using average revenue and average net income provide qualitatively similar results.

[3] The choice of the prior is set to allow large range of values but without much prior information.

[4] The countries are Australia, Canada, Germany, France, Italy, India, Japan, Netherland, Singapore, Spain, Switzerland, the United Kingdom, and the United States.

[5] The measure is calculated by taking an average weighted by the share of gross bilateral cross-border banking exposure (see Online Annex 3.2 of the April 2023 GFSR chapter 3 for technical details).

Online Annex Table 3.2.1 Estimation Results of Generalized Extreme Value Distribution

Model	(1)	(2)	(3)	(4)	(5)	(6)
Locational Parameters	3.91 ***	4.24 **	10.95 ***	13.63 ***	8.95 ***	9.02 ***
	(1.40)	(2.59)	(2.42)	(1.52)	(2.15)	(0.58)
Constant	3.91 ***					
	(1.40)					
Size			8.92 ***	19.48 ***	11.29 ***	12.70 ***
			(5.31)	(3.73)	(5.75)	(8.42)
Telecom Infrastructure			4.30	-9.57 ***	-3.32	-4.47 ***
			(4.05)	(5.59)	(6.07)	(1.44)
Human Capital				6.76 ***		
				(5.06)		
Corporate Governance					-0.03	
					(0.84)	
Geopolitical Proximity						7.66 ***
						(1.72)
Scale Parameters	8.83 ***	5.07 ***	8.12 ***	7.67 ***	7.49 ***	7.06 ***
	(3.06)	(1.52)	(2.13)	(1.10)	(2.23)	(2.06)
Constant	2.12 ***					
	(0.33)					
Size			-5.30	-1.51 ***	-4.07	-3.30 ***
			(4.77)	(0.82)	(6.25)	(0.85)
Telecom Infrastructure			4.13	-2.64	-3.30 **	0.19
			(4.45)	(4.04)	(1.89)	(4.58)
Human Capital				1.68		
				(2.49)		
Corporate Governance					0.43	
					(0.42)	
Geopolitical Proximity						6.54 ***
						(2.37)
Shape	2.12 ***	1.57 ***	1.33 ***	0.88 ***	1.15 ***	1.32 ***
	(0.36)	(0.34)	(0.23)	(0.16)	(0.31)	(0.22)
Fixed Effects	No	Yes	Yes	Yes	Yes	Yes
Number of Data	57	57	46	46	46	46
AIC	542.49	534.55	472.87	442.99	469.33	460.89
BIC	654.49	622.55	534.87	502.99	529.33	520.89

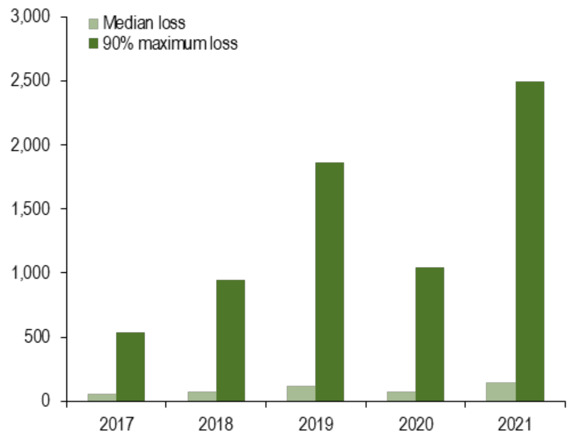
Note: Values are based on posterior mean. Values with branckets represent posterior mean standard deviation. Values with ***, **, and * represent 1%, 5%, and 10% significance based on posterior Bayesian credible interval.
Source: IMF staff calculations.

Aggregated distribution

To construct the aggregated distribution, average locational and scale parameters are computed by taking an average weighted by the share of the sample maximum M_c. The density distribution is shown in Figure 5 (panels 3 and 4) in the main text, and the evolution of the quantiles of the aggregated distribution is shown in Annex Figure 3.2.1. The figure shows that the 90th percentile fluctuates substantially over time.

Online Annex Figure 3.2.1 Estimated quantiles of the maximum cyber loss

(Millions of U.S. dollar)



Source: IMF Staff Calculations.
Note: Estimates are based on the average parameters weighted by the share of sample included in the estimation.

Online Annex 3.3 The effects of cyber incidents on equity prices

Potential losses due to cyber incidents include direct losses but also indirect losses, such as reputational damage leading to a loss of customers or investor confidence, which may not be fully captured by firms' reported direct damages.

To quantify these losses, an event study analysis of the impact of a cyber incident on equity price returns is performed following Kamiya and others (2021) and Amir and others (2018). To analyze the effect of cyber incidents, cumulative abnormal returns (CAR) are estimated as follows:

$$R_{f,c,t} - r_{c,t} = \alpha_f + \beta_f W_{c,t} + \gamma_f \cdot X_{f,t} + e_{f,c,t} \tag{6}$$

where $R_{f,c,t}$ is the logarithmic equity return of firm *f*, $r_{c,t}$ is the logarithmic riskless return in country *c* proxied by the policy rate. The country-level characteristics $W_{c,t}$ include market excess returns ($R^m_{c,t} - r_{c,t}$). $X_{f,t}$ is a vector of control variables, which includes firm *f*'s dividend yields and logarithmic growth of earnings per share (EPS) lagged by one period. Cumulative abnormal returns (CAR) for the targeted firm f are defined as the cumulative sum of the residual $e_{f,c,t}$ as $CAR_{f,T} = \exp\left(\sum_{\tau=0}^{T} e_{f,c,t+\tau}\right) - 1$.

Data

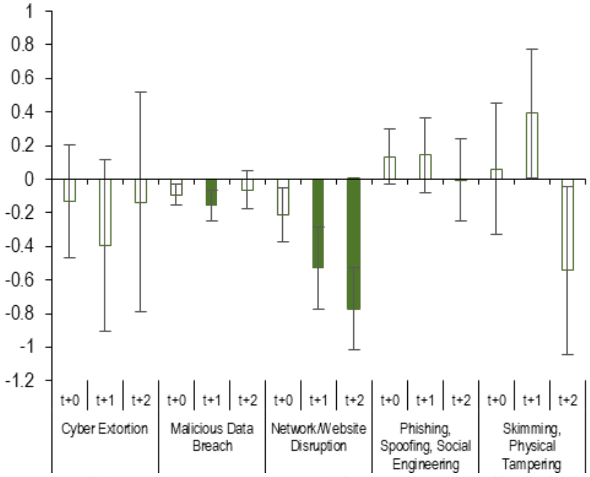
The sample period is January 2012 to May 2023 and includes 836 firm-incident pairs. Firms in public and administrative related service sectors are not included in the sample.[1] Incidents are dropped if they occur within less than 365 days of another incident, and the model is estimated separately for each firm-incident pair with at least 120 days of data points prior to the incident. To avoid weekday effects, weekend returns are dropped, and incidents that happened during the weekends are shifted to the following Monday.

Results

The results in Online Annex Figure 3.3.1. show a significant decline in equity returns for some types of incidents, such as malicious data breaches and network/website disruption. The magnitudes are largest for network/website disruption. Online Annex Figure 3.3.2. shows that the magnitude of the loss is greater for smaller firms. The pattern is particularly clear for malicious incidents.

Online Annex Figure 3.3.1 The Effects of Cyber Incidents on Equity Prices by Type of Incident

(Percentage points)



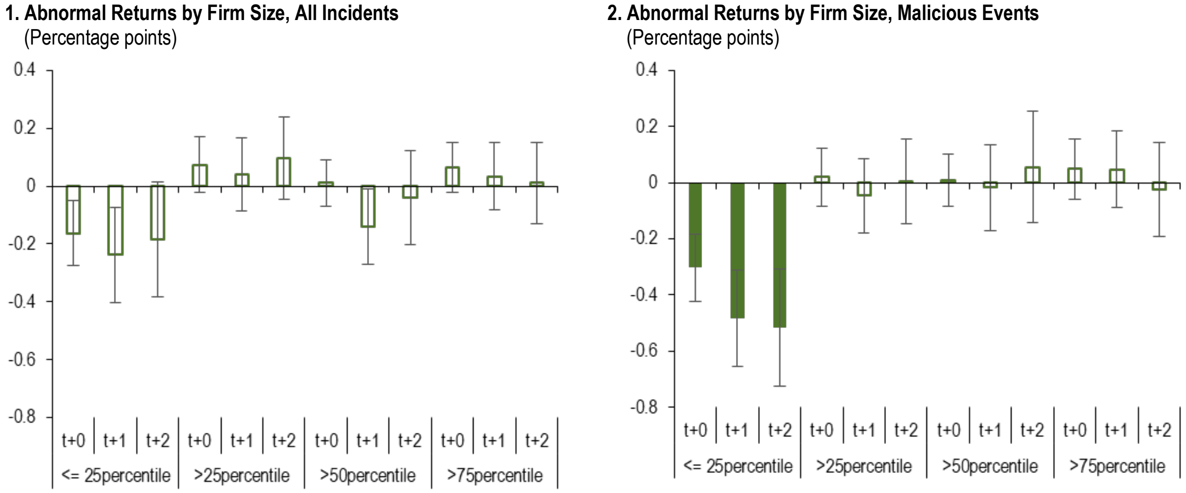
Source: Advisen Cyber Loss Data; Capital IQ; and IMF staff calculations.
Note: Solid bars represent 10% significance level. Whisker lines represent one standard error bands.

Impact on market capitalization

The impact on equity market capitalization is calculated using the estimated cumulative abnormal returns for each incident-firm pair with negative values multiplied by the market capitalization of the same firm one day prior to the incident.

[1] More specifically, firms with SIC code 2351 (public building and related furniture), 4225 (public warehousing and storage), 6111 (federal and federally sponsored credit agencies), 7311 (services-advertising agencies), 7320 (consumer credit reporting, collection agencies), 7361 (employment agencies), 8888 (foreign governments), and 9721 (international affairs) are dropped.

Online Annex Figure 3.3.2 The Effects of Cyber Incidents on Equity Prices by Firm Size


1. Abnormal Returns by Firm Size, All Incidents
(Percentage points)

2. Abnormal Returns by Firm Size, Malicious Events
(Percentage points)

Source: Advisen Cyber Loss Data; Capital IQ; and IMF staff calculations.
Notes: Classification of firm size in the horizontal axis is based on the percentage rank of total assets in U.S. dollar among all sample firms. Solid bars represent 10% significance level. Whisker lines represent one standard error bands

Online Annex 3.4 Drivers of Cyber Incidents

Baseline Model

To examine the drivers of cyber incidents, a probit regression model is employed following Kamiya and others (2021). The baseline model is designed to examine the impact of various firm characteristics on the likelihood of experiencing a cyber incident and is estimated over the period 2013 to 2022. The dependent variable in the model, $Event_{i,c,s,t}$, is a binary variable indicating whether firm *i* in country *c*, sector *s*, in year *t* has experienced a cyber event:

$$Event_{i,c,s,t} = \alpha + \beta X_{i,c,s,t-1} + D_c\gamma_c + D_s\gamma_s + D_t\gamma_t + \varepsilon_{i,c,s,t} \tag{1}$$

Firm characteristics $X_{i,c,s,t}$ include several financial and non-financial metrics that could influence firms' cyber risk profile such as:

- Log (total assets): The natural logarithm of total assets, which accounts for firm size in a non-linear fashion, acknowledging that the relationship between size and cyber events may not be proportional.
- Firm age: The number of years since the firm's establishment, which may correlate with the maturity of its cyber infrastructure.
- Share of asset intangibility: A higher proportion of intangible assets could indicate a greater reliance on digital infrastructure and hence a higher exposure to cyber risks.
- Capex ratio: Capital expenditure ratio to total assets, indicative of the firm's investment in technology which could affect its vulnerability to cyber events.
- Return on Assets (ROA): A profitability measure that could relate to a firm's ability to invest in cybersecurity.
- Leverage: The ratio of debt to total assets, suggesting how leveraged a firm is. Firms with higher leverage may have different risk profiles and priorities for cyber risk management.
- Revenue growth: Year-over-year revenue growth rate, potentially associated with dynamic changes in the firm's operations and exposure to cyber risks.

Country, sector, and year fixed effects are included to control for unobserved characteristics that could influence the outcome variable. Standard errors are clustered at the firm level. By measuring the explanatory variables one year ahead of the event, the model aims to establish a temporal order between the predictors and the outcome, enhancing the argument for a causal interpretation of the results, though causality cannot be definitively established in this framework. Results are consistent with those reported in Kamiya and others (2021).

In order to assess the impact of specific country characteristics on the likelihood of cyber incidents, the model is the augmented with a vector of country variables, $Z_{c,t}$, as follows:

$$Event_{i,c,s,t} = \alpha + \beta X_{i,c,s,t-1} + \delta Z_{c,t} + \gamma_s D_s + \gamma_t D_t + \varepsilon_{i,c,s,t} \tag{2}$$

The country variables are:

- The United Nations Telecommunications Infrastructure Index, to control for the level of technological development.
- A World Bank measure of digital literacy, capturing the extent to which the population possess sufficient digital skills (as of 2019).
- The Maplecroft Cyber Legislation Index, to assess whether countries with more sophisticated legislation on cyber issues are more resilient.
- A Cyberthreat Index (Caldara and Iacoviello, 2022), capturing countries exposure to geopolitical risk and thus attacks from geopolitical adversaries.

Time and sector fixed effects are included in this specification. The coefficient on digital skills is not statistically significant and, thus, is not reported in the main text (Figure 7, panel 1).

Results are qualitatively similar, but weaker when considering financial firms only, probably because of the smaller sample and some firm-level variables being less relevant for financial firms, such as capex. Results for country level variables change only slightly (TII loses its statistical significance). Results are broadly robust to using other measures of geopolitical distance, such as those based on the similarity of foreign policies across country pairs drawing on their voting behavior at the UNGA meetings.

COVID-19 Pandemic, Telework and Governance

The forced and unexpected shift to remote working during the COVID-19 pandemic has been identified as a source of cyber risk, as employees were forced to work more online on potentially less secure networks (Adelmann and Gaidosch 2020). Firms in sectors with a low potential for remote work were likely affected differently from sectors with a high potential. Also, sectors which relied on telework even before the pandemic were likely affected differently from those that had to quickly adapt to working remotely. To analyze these effects, the model is augmented with an interaction term that captures the COVID-19 pandemic period and firms' preparedness to work remotely:

$$Event_{i,c,s,t} = \alpha + \beta X_{i,c,s,t-1} + \tau dummy2020_t + \theta TW_s + \varphi dummy2020_t TW_s + \gamma_c D_c + \varepsilon_{i,c,,s,t} \qquad (3)$$

where $dummy2020_t$ takes the value one for the years 2020-2022, and TW_s is a variable representing low, medium, and high teleworkability based on the share of the workforce which can work remotely by NAICS sectors (as in Dingel and Nieman 2020). Online Annex Table 3.4.1 shows the share of the workforce capable of working remotely by sector, and the classification into the three groups used in the analysis.[2] The model includes country fixed effects but no time or sector fixed effects. Results are shown in Chapter Figure 7, panel 2 and are qualitatively similar when using the index of teleworkability directly and when using a dummy just for 2020.

Effect of past cyber incidents on vulnerability

Being subject to a cyber incident may lead to behavioral changes in the affected company, such as more robust cybersecurity practices. It could also expose companies as vulnerable to cyberattacks. To study the impact of cyber incidents on future cyber vulnerability, the following probit model is estimated:

$$Event_{i,t} = \alpha + \delta Past\_event_{i,t} + \gamma_i D_i + \gamma_t D_t + \varepsilon_{i,t} \qquad (4)$$

where $Past\_event_{i,t}$ takes the value one if a company experienced a cyber incident in the previous two years. $D_i$and D_t are firm and year fixed effects, respectively. Results are shown in Chapter Figure 7, panel 4 and are qualitatively unchanged when considering cyber events in the previous year only or when considering only malicious cyber events as explanatory variable.[3]

Effect of past cyber incidents on Governance

To investigate potential channels through which cyber incidents might lower the future likelihood of cyber events, a probit regression with the change in cyber security expertise at the board level as dependent variable and past cyber incidents as explanatory variable was estimated:

$$Cyber\_exp_{i,t} = \alpha + \delta P_{Event_{i,t-1}} + \gamma_i D_i + \gamma_t D_t + \varepsilon_{i,t} \qquad (5)$$

where, $Cyber\_exp_{i,t}$ is a binary variable capturing if firm *i* increased the number of board members with cyber experience at time *t* (constructed from Orbis by matching specific cybersecurity-related terms to the contents of the executives' biographies).[4] The model is estimated using firm and time fixed effects.

[2] The measure captures the share of jobs that can be done at home in each 2-digit NAICS sector. It is computed using the authors' O*NET-derived classification of occupations that can be done at home and the occupational composition of each 2-digit sector's employment by 6-digit SOC in the BLS's 2018 Occupational Employment Statistics. Table 3.4.1 presents the breakdown of each sector by the degree of teleworkability.

[3] Malicious cyber events account for 68.7 percent of all cyber incidents in the sample.

[4] Only senior board members were included in the analysis. The search over biographies included the following keywords: Cybersecurity; Information Security; Information Assurance; Cybersecurity Governance; Data Privacy; Data Protection; Network Security; Cyber Threat

Continued

Results are shown in Chapter Figure 7, panel 4. Of the cyber-related governance variables, the number of board members with cyber experience turns out to be statistically significant. The sign of the estimated coefficients on the other variables was consistent with cybersecurity improving after cyberattacks, but those were not statistically significant, possibly due to the small number of observations.

Online Annex Table 3.4.1 Sectors by “Teleworkability” Group

Sector	Share of workforce	Teleworkability Group
Educational Services	0.83	High
Professional, Scientific, and Technical Services	0.80	High
Management of Companies and Enterprises	0.79	High
Finance and Insurance	0.76	High
Information	0.72	High
Wholesale Trade	0.52	Medium
Real Estate and Rental and Leasing	0.42	Medium
Federal, State, and Local Government	0.41	Medium
Utilities	0.37	Medium
Other Services (except Public Administration)	0.31	Medium
Administrative and Support and Waste Management and Remediation Services	0.31	Medium
Arts, Entertainment, and Recreation	0.30	Medium
Mining, Quarrying, and Oil and Gas Extraction	0.25	Low
Health Care and Social Assistance	0.25	Low
Manufacturing	0.22	Low
Transportation and Warehousing	0.19	Low
Construction	0.19	Low
Retail Trade	0.14	Low
Agriculture, Forestry, Fishing and Hunting	0.08	Low
Accommodation and Food Services	0.04	Low

Source: Dingel and Nieman (2020).

Intelligence; Cloud security; Malware; CISSP (Certified Information Systems Security Professional); CISM (Certified Information Security Manager); CISA (Certified Information Systems Auditor); CRISC (Certified in Risk and Information Systems Control); CGEIT (Certified in the Governance of Enterprise IT); GSEC (GIAC Security Essentials); CERT (Carnegie Mellon Certificate in Cybersecurity Oversight); CCSP (Certified Cloud Security Professional); CEH (Certified Ethical Hacker); CISO (Chief Information Security Officer); CTO (Chief Technology Officer); IT Director; IT Auditor; Data Privacy; Information Security Officer; Security Engineer; Network architect; Systems architect.

Online Annex 3.5 The Cyber Threat Landscape in the Financial Sector

Cybersecurity Ratings in the Financial Sector

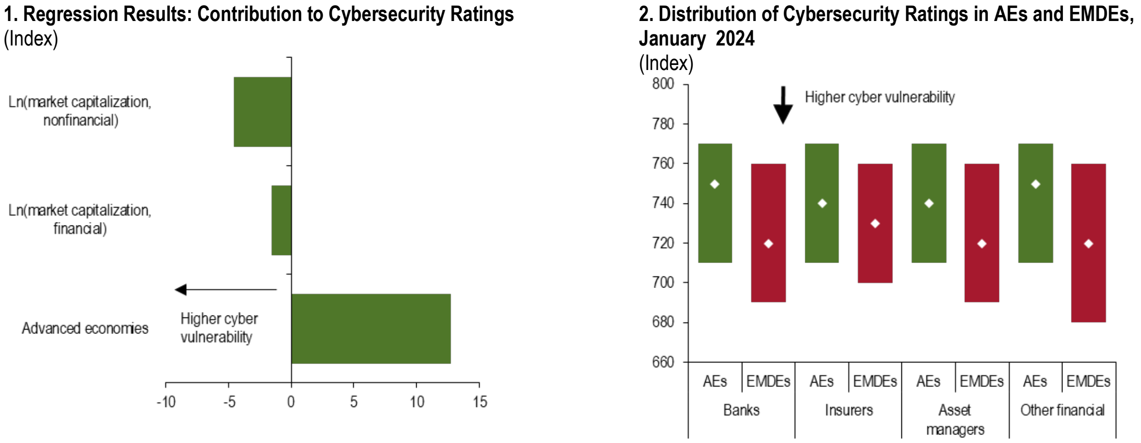
To better understand the determinants of Bitsight Cybersecurity ratings, the following cross-sectional regression model is estimated:[1]

$$y_i = \alpha + \beta_S + \gamma_1 D_f\, MC_i \; + \gamma_2 (1 - D_f\,) MC_i \; + \delta D_{AE} \; + \varepsilon_i, \tag{1}$$

where y_i represents firm *i*'s cybersecurity rating as of January 2024, β_S are sector fixed effects defined at the 4-digit SIC code level, MC_i represents the logarithm of market capitalization and D_f is a dummy variable equal to one if the firm is in the financial sector based on SIC codes, and zero otherwise. D_{AE} is a dummy variable equal to one if the firm is in advanced economies (AEs), and zero otherwise. The total number of observations in the sample is 20,649 and standard errors are heteroskedasticity-consistent.

Online Annex Figure 3.5.1 (panel 1) shows that cybersecurity ratings generally decline as market capitalization increases, for both financial and non-financial firms, suggesting that larger firms tend to receive lower ratings due to their greater exposure to cyber risk.[2] Additionally, the ratings tend to be higher for firms located in AEs. Moreover, Online Annex Figure 3.5.1 (panel 2) indicates that, across all subsectors, cybersecurity ratings for financial firms in AEs tend to be higher than those in EMDEs.

Online Annex Figure 3.5.1 Properties of Cybersecurity Ratings in the Financial Sector



Sources: Bitsight; Orbis; and IMF staff calculations.
Notes: In panel 1, solid bars represent significance at the 10 percent level. In panel 2, diamonds indicate the median and boxes indicate the interquartile range of the ratings across the financial institutions in the subsector.

Cybersecurity Preparedness in the Financial Sector

According to Figure 3.8.1, the cybersecurity ratings of globally systemically important banks (G-SIBs) are lower than those of other financial firms, implying lower cybersecurity preparedness or higher exposure. To explore the role of cybersecurity preparedness, the following indicators are examined:

- The MSCI **Privacy and Data Security Management Score** which evaluates a company's management practices in this domain.[3]
- The Refinitiv Datastream **Corporate Governance Score** which measures a company's commitment and effectiveness towards following best practice corporate governance principles.

[1] As of January 2024, Bitsight ratings were available for 305,667 firms, including 28,900 financial firms. Among these financial firms, there were 10,263 banks, 2,866 insurers, and 3,581 asset managers. The ratings cover 275,209 firms in Advanced Economies (AEs) and 30,458 in Emerging and Developing Market Economies (EMDEs).

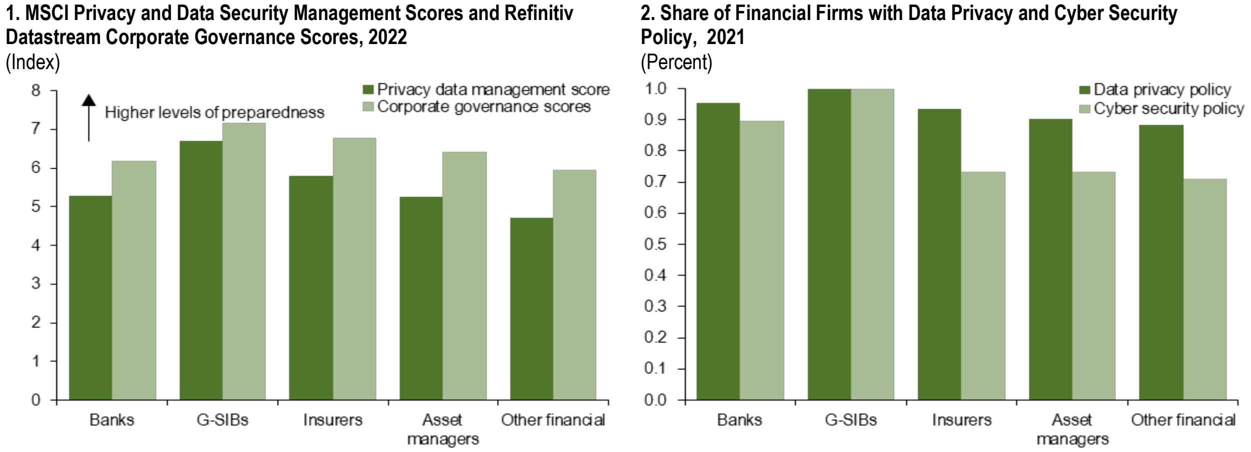
[2] Additional analysis suggests that G-SIB's cybersecurity ratings cannot be solely explained by their size.

[3] The score takes into account various factors, including the scope of a company's data protection policy, individual rights, data breach response plans, audits of information security policies, access control, data minimization, employee training, executive responsibility, and certifications to recognized standards.

- Whether a firm has a data privacy policy and a cyber security policy in place.

Online Annex Figure 3.5.2. illustrates the indicators by financial subsector.[4] Notably, G-SIBs exhibit higher Privacy and Data Management Scores and Corporate Governance Scores compared to other banks and other financial firms. The figure also indicates that G-SIBs are more likely to have data privacy and cyber security policies in place than other banks and financial firms. This suggests that G-SIBs have relatively high levels of cybersecurity preparedness, but their Bitsight Cybersecurity Ratings imply that this preparedness may not be sufficient relative to G-SIBs' greater exposure to cyber risk.

Online Annex Figure 3.5.2 Properties of Cybersecurity Ratings in the Financial Sector



1. MSCI Privacy and Data Security Management Scores and Refinitiv Datastream Corporate Governance Scores, 2022
(Index)

2. Share of Financial Firms with Data Privacy and Cyber Security Policy, 2021
(Percent)

Sources: MSCI; Refinitiv Datastream; and IMF staff calculations

Concentration in the Financial Sector

Online Annex Figure 3.5.3 shows the market concentration of banks, major insurers, and major asset managers over time. Concentration in the banking sector—both domestically and globally—has stayed relatively stable over the past two decades when considering the market shares of the largest three or five banks (panels 1-4). Global concentration in the insurance sector has remained stable as well (panel 5) while there has been an increase in the concentration of the global asset management sector (panel 6).

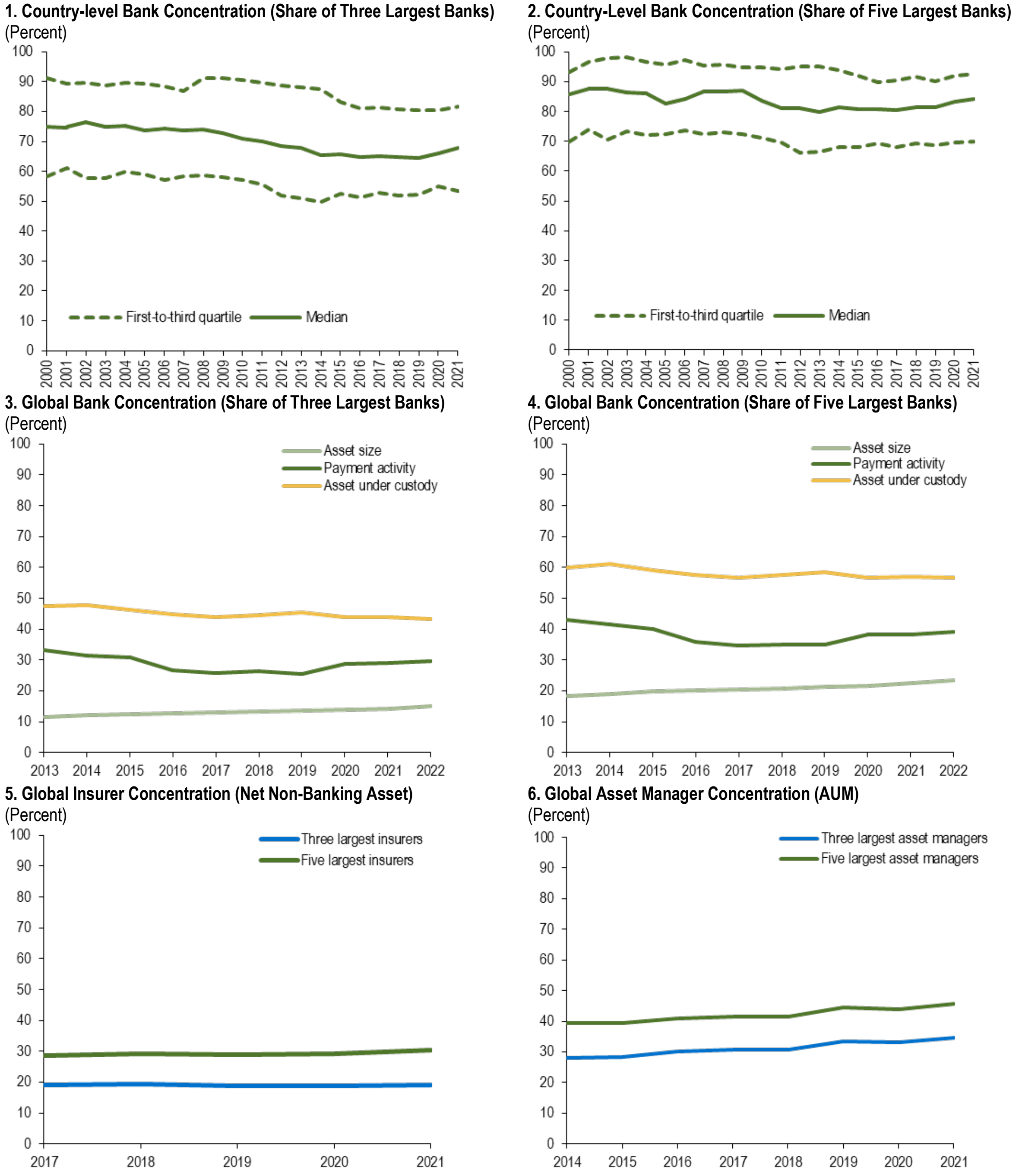
Exposure to Cyber Risk from IT Providers in the Financial Sector

The Chapter highlights potential risks from financial firms sharing the same third-party IT providers. Online Annex Figure 3.5.4 (panel 1) illustrates that such connections could also create cross-border exposures with approximately 50-60 percent of IT providers servicing financial firms internationally.

With major financial firms being exposed to cyber risk through their IT providers, the cybersecurity of these providers is of particular interest. Online Annex Figure 3.5.4 (panel 2) shows that cybersecurity ratings of IT providers are similar across the different financial subsectors. When compared to the sectors that purchase their services, G-SIBs' IT providers exhibit higher cybersecurity levels, while ratings of the providers of major insurers and asset managers are slightly lower.

[4] The samples for Privacy and Data Security Management (Corporate Governance) Score consist of 624 (631) banks, 168 (169) insurers, 187 (195) asset managers, and 242 (254) other financial firms. The samples for existence of data privacy and cyber security policies are composed of 152 banks, 15 insurers, 82 asset managers, and 86 other financial firms.

Online Annex Figure 3.5.3 Local and Global Concentration of Major Financial Firms



1. Country-level Bank Concentration (Share of Three Largest Banks)
(Percent)

2. Country-Level Bank Concentration (Share of Five Largest Banks)
(Percent)

3. Global Bank Concentration (Share of Three Largest Banks)
(Percent)

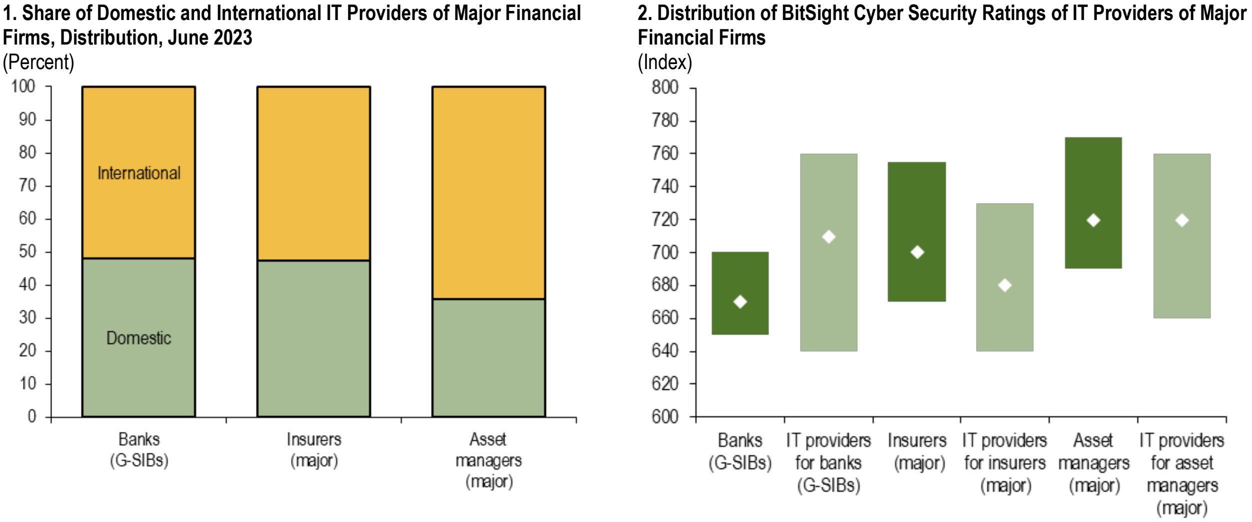
4. Global Bank Concentration (Share of Five Largest Banks)
(Percent)

5. Global Insurer Concentration (Net Non-Banking Asset)
(Percent)

6. Global Asset Manager Concentration (AUM)
(Percent)

Sources: AM Best; BIS; Bitsight; FactSet; Orbis; P&I/Thinking Ahead Institute; and IMF staff calculations.
Notes: In panels 1 and 2, the median and the first-to-third quartile of all sample countries in each year. In panels 3 and 4, the sample banks are 75 largest banks which are included in the samples of G-SIB assessment in each year. 'Asset size' in panels 1, 2 and panels 3, 4, respectively, indicate total asset and total exposures. In panel 5, the sample insurers are 25 largest insurers in rankings by AM best, and in panel 6, the sample asset managers are 25 largest asset managers in rankings by P&I/Thinking Ahead Institute.

Online Annex Figure 3.5.4 Properties of Financial Sector IT Providers



Sources: Bitsight; FactSet; Orbis; and IMF staff calculations.

Notes: Online Annex 3.1 indicates the definition of major financial firms. Third-party IT providers are defined as information technology services, internet software/services, packaged software, data processing service, computer peripherals, and computer processing hardware. Diamonds indicate the median and boxes indicate the interquartile range of the ratings across the financial institutions in the subsector as of January 2024.

Online Annex 3.6 Cyberattacks and Bank Deposits

Response of Wholesale and Retail Deposits to a Malicious Cyber Incident

To examine the impact of malicious cyber incidents at US banks on their wholesale[1] and retail deposit flows, the analysis estimates the following local projection model using data from 2014q1 to 2022q4:[2]

$$l\,n(y_{i,t+h}) - l\,n(y_{i,t-1}) = \alpha_{i,h} + \beta_{t,h} + \gamma_h D_{i,t} + \delta_h control_{i,t} + \varepsilon_{i,t,h} \qquad (1)$$

for $h = 0,1,\dots,8$, where $y_{i,t}$ represents the amount of bank *i*'s wholesale/retail deposit in period *t*, and $D_{i,t}$ is a binary variable ('malicious cyber incident dummy') equal to one if bank *i* experienced a malicious cyber incident(s) within period *t* and zero otherwise. Malicious cyber incidents are defined as in Online Annex 3.1 (date is the Advisen 'first notification date') and occur in around 1 percent of bank-quarter observations. To absorb the impact of business and financial cycles as well as bank characteristics (e.g., trends of deposits), the following control variables are considered: i) bank-level fixed effect $\alpha_{i,h}$, ii) period effect $\beta_{t,h}$, iii) two period lag of deposit flows ($l\,n(y_{i,t-1}) - l\,n(y_{i,t-2})$, $ln(y_{i,t-2}) - l\,n(y_{i,t-3})$), and iv) a malicious cyber incident dummy variable ($D_{i,t-1}$, $D_{i,t-2}$).[3] The estimates of γ_h show the cumulative response of all banks' deposit flows to malicious cyber incidents. Standard errors are clustered at the bank level.

To further explore the heterogeneity of the impact of cyber incidents on banks' deposit flows, model (1) is extended as follows:

$$l\,n(y_{i,t+h}) - l\,n(y_{i,t-1}) = \alpha_{i,h} + \beta_{t,h} + \gamma_{a,h} D_{i,t,a} + \gamma_{b,h} D_{i,t,b} + \delta_h control_t + \varepsilon_{i,t,h} \qquad (2)$$

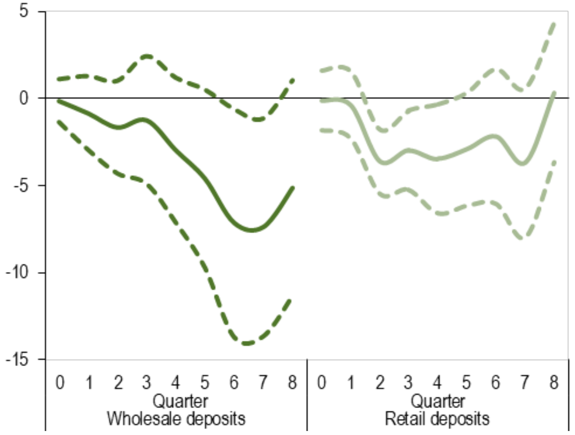
where$D_{i,t,a} = d_{i,t,a}\, D_{i,t}$ and $D_{i,t,b} = (1 - d_{i,t,a}) D_{i,t}$ and $d_{i,t,a}$ represents a dummy variable which takes the value one if

- the amount of bank *i*'s domestic deposits in $t-1$ is smaller than the two-third percentile. In this case, the estimates of $\gamma_{a,h}$ show the cumulative response of smaller banks' deposit flows to malicious cyber incidents.
- the number of affected counts is above 500. In this case, the estimates of $\gamma_{a,h}$ show the cumulative response of all banks' deposit flows to malicious cyber incidents with a larger number of affected accounts.

The estimation results of the first specification are shown in the main text. Online Annex Figure 3.6.1 shows that for incidents with a large number of affected accounts the negative response of deposits becomes modestly stronger than panel 1 of Figure 9.

Online Annex Figure 3.6.1 Response of Wholesale and Retail Deposits to a Cyberattack with a Larger Number of Affected Counts at US Banks, 2014-2022

(Deviation from the baseline, percent)



Sources: Advisen Cyber Loss Data; Federal Financial Institutions Examination Council; and IMF staff calculations.
Note: Solid lines represent estimates of the response of banks' deposits to the occurrence of malicious cyber incidents in a given quarter. Dotted lines indicate the 90 percent confidence intervals (cross-section cluster robust standard errors).

[1] As indicated in the main text, "wholesale deposits" are defined as deposits from private, non-depository institutions, but the results remain almost unchanged if deposits from depository institutions are included in "wholesale deposits."

[2] The variables which are necessary to calculate wholesale and retail deposits are only available from 2014q1.

[3] The variables, except for the malicious cyber incident dummy, are obtained from the Call Report database prepared by Federal Financial Institutions Examination Council.

Reverse Outflow Rates

Bank *i*'s reverse outflow rate ($R_{i,t}$) in period *t* is defined as the rate at which the bank's liquidity coverage ratio ($LCR_{i,t}$) would drop below the 100 percent regulatory requirement. Specifically, $R_{i,t}$ is computed as:

$$LCR_{i,t} = \frac{HQLA_{i,t} - R_{i,t} * Deposit_{i,t}}{Net\ outflows_{i,t} - R_{i,t} * Run\ off_{i,t} * Deposit_{i,t}} * 100 = 100$$
$$\Leftrightarrow\ R_{i,t} = \frac{HQLA_{i,t} - Net\ outflows_{i,t}}{Deposit_{i,t}\left(1 - Run\ off_{i,t}\right)} \tag{3}$$

where $HQLA_{i,t}$ represents the amount of high-quality liquid assets held by bank *i* in period *t*, and $Net\ outflows_{i,t}$ is the hypothetical total net cash outflow over the next 30 days, both of which are calculated based on current LCR regulation in each jurisdiction. $Deposit_{i,t}$ indicates the amount of unsecured wholesale or retail deposits in the bank which mature within 30 days or have undetermined maturity. $Run\ off_{i,t}$ represents the average run-off rates applied to the deposit, calculated based on current LCR regulation in each jurisdiction. Unsecured wholesale deposit is defined as the sum of operational and non-operational deposits in the category of unsecured wholesale funding, and retail deposit corresponds to the sum of retail deposits and deposits from small business customers, including both stable and less stable deposits. As seen in equation (3), the reverse outflow rate is increasing in $HQLA_{i,t}$ and $Run\ off_{i,t}$ while it is decreasing in $Deposit_{i,t}$.[1] The sample banks are those which participated in the 2022 G-SIB assessment and disclosed detailed LCR calculations (88 global banks).[2]

[1] Deposit outflows would force banks to sell HQLA while, at the same time, also decreasing the amount of hypothetical outflows assumed in the LCR calculation. Note that hypothetical inflows are assumed to remain unchanged.

[2] The LCR data of 80 banks, 6 banks, and 2 banks are, respectively, as of September 2023, June 2023, and December 2022.

Online Annex 3.7 IMF Cybersecurity Survey

In 2023 (2021) the IMF surveyed 74 (53) EMDEs on cybersecurity preparedness (Online Annex Table 3.7.1). The surveys covered 43 questions related to governance and strategy, cyber regulation and supervision, monitoring, response and recovery, information sharing and incident reporting, cyber deterrence, financial stability analysis, and continuous learning and capacity development. The full list of survey questions is provided in Online Annex Table 3.7.2.

Online Annex Table 3.7.1 IMF Cybersecurity Survey Respondents

2021	2023
Angola, Armenia, Aruba, Bangladesh, Benin, Bolivia, Bosnia And Herzegovina, Bulgaria, Cambodia, Cape Verde, Comoros, Costa Rica, Democratic Republic of The Congo, Djibouti, Dominican Republic, Ecuador, El Salvador, Fiji, Georgia, Guatemala, Honduras, India, Indonesia, Iraq, Jordan, Kenya, Laos, Libya, Madagascar, Malaysia, Maldives, Marshall Islands, Montenegro, Morocco, Mozambique, Namibia, Nepal, Nicaragua, Pakistan, Philippines, Republic of Moldova, Republic of North Macedonia, Romania, Rwanda, Sudan, Suriname, Tanzania, Tonga, Trinidad And Tobago, Uganda, Uruguay, Vietnam, Zimbabwe	Albania, Angola, Armenia, Bangladesh, Barbados, BCEAO, BCEAO - SENEGAL, BCEAO Benin, Belize, Bhutan, Bolivia, Bulgaria, Cabo Verde, Cambodia, Comoros, Congo, Costa Rica, Democratic Republic of the Congo, Djibouti, Dominican Republic, Eastern Caribbean Currency Union, Equatorial Guinea, El Salvador, Eswatini, Ethiopia, Gabon, Georgia, Ghana, Guatemala, Guyana, Honduras, India, Indonesia, Jamaica, Jordan, Kosovo, Kyrgyz Republic, Lao PDR, Lesotho, Liberia, Libya, Madagascar, Malawi, Malaysia, Maldives, Mauritania, Mongolia, Morocco, Mozambique, Namibia, Nepal, North Macedonia, Pakistan, Papua New Guinea, Philippines, Republic of Burundi, Republic of Guinea, Republic of Moldova, Republic of the Marshall Islands, Republic of Uzbekistan, Rwanda, S.Tomé e Príncipe, Sierra Leone, Solomon Islands, Tajikistan, The Federal Republic of Somalia, The Gambia, Tonga, Tonga, Uganda, Ukraine, Uruguay, Yemen, Zambia

Online Annex Table 3.7.2 IMF Cyber Survey Questions

Governance and strategy

Q. No	Question and multiple-choice answers
1	Does your jurisdiction have a national cyber strategy, which includes the financial sector? a) Yes, we have a national cyber strategy, which includes the financial sector. b) No but we, as the central bank or supervisory agency, are currently working on a government-driven national cyber strategy, that is expected to be endorsed in the next 12 months. c) No, but the government is developing a strategy that is expected to be finalized in the next 12 months (without active involvement of the central bank / supervisors) d) No, we do not have a national cyber strategy, although there are ongoing discussions on whether we should develop such a strategy. e) No.
2	Does your central bank or supervisory agency have a cyber strategy for the financial sector? a) Yes, and it is integrated into the national cyber strategy. b) Yes, however, it is separate and not connected to the national cyber strategy. c) No, but we are currently developing one and expect to publish it within the next 12 months. d) No.
3	Did the Board of your central bank or supervisory agency approve the central bank and/or supervisory agency's cyber strategy for the financial sector and does it regularly monitor its progress in implementation? a) Yes b) No
4	Does your jurisdiction have formalized governance arrangements in place to manage cyber risk? a) Yes, our jurisdiction has a formalized governance structure in place at government level, which delegates to the central bank and/or the supervisory agencies the responsibility for mitigating cyber risk in the financial sector. b) Yes, there is a formalized governance structure in place within the central bank and/or supervisory agencies, however, the governance arrangements are not connected with other governmental agencies and other sectors. c) No, but there is ongoing work at government level expected to be finalized in the next 12 months d) No, but the central bank / supervisory agency is currently working on establishing formalized governance arrangements within the central bank and/or supervisory agency in the next 12 months. e) No, not at governmental level nor within the central bank and/or supervisory agency. If there is ongoing work to develop such arrangements, it is expected to take longer than 12 months.
5	What is the mandate of the central bank and/or supervisory agency with regards to cyber risk? (Select all that apply) The central bank/ supervisory agency is responsible for cyber risk as part of: • prudential supervision of financial institutions • oversight of financial market infrastructures • financial stability • operation of the RTGS system • operating the financial CERT or similar activity • carrying out cyber exercises and coordinating testing frameworks
6	The central bank and supervisory agency have a formalized working relationship with each other, which includes sharing of information for financial stability reasons? • Yes • No • Not applicable (the central bank is also responsible for supervision)

Cyber regulation and supervision

Q. No	Question and multiple-choice answers
7	Does your jurisdiction have a dedicated and published cybersecurity or technology risk management regulation for the financial sector? a) Yes, we have a dedicated cybersecurity/technology risk management regulation, which has been published. b) No, but we are currently developing a cybersecurity/technology risk management regulation, which will be published in 12 months c) No, we do not have a dedicated cybersecurity or technology risk management regulation but include this risk area as part of our operational or risk management regulation. d) No
8	Does your cybersecurity regulation apply to: • Banks • FMIs • Insurance companies

	• Non-banks • Third party providers • None of the above, as we do not have cybersecurity regulation **(Select all that apply)**
9	Does your jurisdiction have a dedicated and published data privacy regulation? a) Yes. b) No, but we are currently developing one, which will be published in 12 months c) No
10	How is the supervisory architecture organized within your jurisdiction? a) We have a specialized Cyber Risk Unit as part of the Supervision Department. b) We have a specialized Cyber Risk Unit outside the Supervision Department. c) We leverage the skill set of our IT department to conduct ICT / cyber examinations, but these are coordinated by the Supervision Department d) We do not have a specialized Cyber Risk Unit as of now, but we are planning to have one soon. We do not take support from the IT Department and ICT / cyber risk work is handled by generalists in an ad-hoc manner.
11	How are ICT / cyber risk concerns conveyed to the supervised entity? a) ICT / Cyber risk is part of the Examination Report issued to the supervised entity. b) While major ICT / cyber risk observations are included in the main Examination report, a separate ICT / cyber risk report is issued to the supervised entity. c) ICT / Cyber risk observations are not part of the main Examination report; but an ICT / cyber risk examination report is issued separately to the supervised entity. d) ICT / cyber risk assessments do not lead to the issue of any report, but major actionable items are conveyed by way of a supervisory letter. e) ICT / cyber risk observations are discussed with the supervised entity but are not conveyed through the Examination Report nor through supervisory letters.
12	What are the methods deployed for onsite supervision of cyber risk? a) We have a full range of approaches (full scope examination, limited scope examination, short visits and thematic reviews), as well as the legal powers to mandate external audits and forensic investigations. b) We conduct onsite supervision (full scope or limited scope examination). Thematic reviews are generally not used but we have legal powers to mandate external audits or forensic investigations. c) We conduct predominantly thematic reviews. Full scope examinations are rare, but we do limited scope examinations at times. We have legal powers to mandate external audits or forensic investigations. d) We require an external audit of cyber preparedness of banks/FMIs on a yearly basis. We have limited capacity to conduct onsite examinations. e) We do not conduct onsite examinations. We do not have the legal powers to mandate external audits or forensic investigations.
13	What are the arrangements for offsite supervision of cyber risk? a) We collect a full range of offsite information that pertains to ICT / cyber. We carry out analysis of such data with a focus to identify material risks faced by the individual entity as well as the system as a whole, and we provide key inputs to the onsite team. b) We have a separate offsite function which collects data, which we analyze regularly. c) We have just established an offsite function and currently collect very limited information. We plan to strengthen the offsite function significantly in the coming year. d) We do not have a dedicated offsite function, but we have the capability to collect ad-hoc information at a short notice. e) At this juncture we do not have any plan to set up an offsite function for ICT / cyber.
14	Do you have powers to conduct an onsite inspection of third-party providers, if necessary? a) Yes. b) No. c) Unclear

Monitoring, response and recovery

Q. No	Question and multiple-choice answers
15	How do supervisors keep informed about cybersecurity risks and emerging threats ("threat landscape")? a) Based on individual initiative and research, mostly uncoordinated b) Based on informally agreed responsibilities within the supervisory team c) Based on formally assigned job responsibilities, not full-time d) Relying on a full-time threat intelligence officer or similar resource
16	What information sources do you use to understand the threat landscape? **(Select all that apply)** a) Freely available content on the web (blogs, news, etc.)

	b) Paid subscription to at least one threat intelligence or information sharing service c) Internal analysis of regulatory reporting d) Meetings with key stakeholders at supervised institutions
17	Did you publish updates in the last two years to your cybersecurity regulation in response to changes in the threat landscape? a) Yes, specifically in the areas of ___________________________ b) No c) We don't have specific cybersecurity regulation
18	How do you deal with cybersecurity incidents occurring at supervised institutions? **(Select all that apply)** a) Analyzing mandatory reporting of cyber incidents b) Off-site monitoring the response and recovery activities of the institution c) On-site involvement in response and recovery without taking control (i.e., advisory role) d) On-site direction and control of response and recovery activities e) We have not established the process yet
19	What is your approach to cybersecurity testing and exercises? (Such as penetration tests, red teaming, and effectiveness of cyber incident response and crisis management exercises.) a) Tests and exercises are encouraged but currently not required b) Tests and exercises are required but there is no further guidance c) Tests and exercises are required and there is further guidance (e.g., on scope, coverage, periodicity, or methods) d) There is a mandatory cybersecurity testing regime that is actively managed by the authorities

Information sharing and incident reporting

Q. No	Question and multiple-choice answers
20	Do you have a cyber information and intelligence sharing arrangement in place in your financial sector? a) Yes, the financial entities in the sector systematically share information and intelligence with each other. b) No, but all financial entities or most financial entities are part of an information sharing network, such as Financial Services Information Sharing and Analysis Center (FS-ISAC).. c) No, but we are developing an information and intelligence sharing network with the financial sector. This will be operational in the next 12 months. d) No, we are not aware of any such arrangement.
21	Are you, as a central bank or supervisory agency, a member of industry-wide information-sharing groups (e.g. national computer emergency response team (CERT), FS-ISAC or the information sharing arrangement cited in the question before)? a) Yes b) No
22	Does your authority have information-sharing arrangements with financial authorities in other jurisdictions (e.g. foreign authorities)? a) Yes b) No
23	Does your authority have information-sharing arrangements with authorities across sectors within your jurisdiction? a) Yes b) No
24	Do you have a cyber incident reporting regime in place? a) Yes, we have a dedicated cyber incident reporting regime and financial institutions are required to report incidents by law or regulation. b) No, we don't have a dedicated and specific cyber incident reporting regime in place but financial institutions are required to report incidents as part of their operational risk requirements. c) No
25	Have you established (a) a taxonomy of cyber incidents (to designate them) and (b) a categorization of their severity to measure their importance? a) Yes, both (a) and (b) b) Only (a) c) Only (b) d) No, neither
25	Indicate which of the following you have established. a) A taxonomy of cyber incident (to designate them) b) A categorization of their severity to measure their importance c) None of the above
26	Do you have an established methodology for determining the materiality (i.e. the impact and severity) of a cyber incident that is used in cyber incident reporting?

	a) Yes b) No c) Not applicable (do not have a cyber incident reporting framework)
27	Do you issue a cyber incident reporting template to your supervised institutions? a) Yes b) No c) Not applicable (do not have a cyber incident reporting framework)
28	Does the operator and participants of a wholesale payment system or a messaging network collaborate in support of information-sharing and ongoing education and awareness about evolving endpoint security risks and risk controls? a) Yes b) No
29	Does the operator and participants of a wholesale payment system or a messaging network leverage existing cyber security working groups to incorporate fraud-related elements of the strategy to reduce the risk of wholesale payments fraud related to endpoint security into their plans? a) Yes b) No

Cyber deterrence

Q. No	Question and multiple-choice answers
30	Is there a cybercrime regulation in place in your jurisdiction, which sets out the different types of cybercrime, the role and responsibilities of law enforcement authorities, the processes for prosecuting cyber criminals and the punishment to be meted out to such criminals? a) Yes. b) No.
31	What are the arrangements for dealing with cyber incidents with the help of law enforcement authorities? a) Law enforcement authorities have specialized cyber units and are responsible for combatting, preventing, disrupting, investigating and prosecuting cybercrime and cyber criminals. The law enforcement authorities have a close working relationship with the central bank and financial entities. b) Law enforcement authorities have specialized cyber units and are responsible for combatting, preventing, disrupting, investigating and prosecuting cybercrime and cyber criminals. The law enforcement authorities do NOT have a close working relationship with the central bank and financial entities. c) There are no specialized cyber-related law enforcement arrangements in place.
32	What arrangements are there between law enforcement authorities, the central bank and financial entities to ensure prosecution of cyber criminals? a) There is clear guidance and processes between law enforcement authorities, the central bank and financial entities on how to report cybercrime, retain digital evidence and to transfer this evidence to aid prosecution of cyber criminals. b) There is clear guidance and processes between law enforcement authorities and financial entities on how to report cybercrime, retain digital evidence and to transfer this evidence to aid prosecution of cyber criminals. The central bank is not involved in this process. c) There is no clear guidance and processes between law enforcement authorities, the central bank and financial entities on how to report cybercrime, retain digital evidence and to transfer this evidence to aid prosecution of cyber criminals.
33	What coordination is there in place with CERT and law enforcement authorities? a) The central bank runs the financial sector CERT (FinCERT) and coordinates with law enforcement agencies effectively. b) The FinCERT is a separate entity not run by the central bank. The central bank and CERT / Fin CERT coordinate their activities well. c) The central bank coordinates effectively with the CERT. There is no Fin CERT in the country. d) The central bank rarely gets in touch with the CERT. Activities are not well coordinated. e) There is no CERT in the country.

Financial stability analysis

Q. No	Question and multiple-choice answers
34	Have you developed a "cyber map" that identifies the main technologies, services, and connections between financial sector institutions, service providers, and in-house or third-party systems? a) Yes, we have developed a cyber map of our financial sector and use it as a reference for supervisors to identify key vulnerabilities and allocate resources. b) Not yet, however, we have collected the relevant information required to produce a cyber map, which we intend to complete in the next 12 months. c) No, and we do not have the requisite information available to produce a cyber map.

35	Do you conduct quantitative analysis of cyber risk in your jurisdiction? a) Yes, we collect data on frequency and loss from cyberattacks and have a methodology to quantify potential future losses. b) No, we do not collect the relevant data and do not have a methodology to quantify cyber risk and potential future losses stemming from cyberattacks.
36	Does your stress test program include cyber risk? a) Yes. b) No.
37	What proportion of your financial sector has migrated part of or all of their functions to cloud service providers? a) Most financial institutions. b) Several financial institutions. c) The minority of financial institutions. d) This information is not available

Continuous learning and capacity development

Q. No	Question and multiple-choice answers
38	What is the approach to strengthening cyber risk supervisory capacity? a) There is no formalized approach yet; decisions are made as needs arise b) There is a general capacity development plan that is implicitly applicable to cyber risk supervision as well c) There is a capacity development plan that is specific to cyber risk supervision
39	What approaches are used to raise cybersecurity awareness in the financial sector and the public at large? (Select all that apply) a) Workshops with key stakeholders b) Participating in, or encouraging public-private partnerships c) Interviews, speeches, and publications d) Co-operation with academia
40	Which cybersecurity training options are available for supervisors? (Select all that apply) a) Free webinars and on-line courses b) Certification training and exams (e.g., CISA, CISSP, and so on) subsidized by the authority c) Academic programs (e.g., undergraduate, graduate, or post-graduate) subsidized by the authority
41	Is an academic degree in IT required to become a cyber risk supervisor? a) Yes b) No
42	Do you require cyber risk supervisors to obtain and maintain relevant professional certifications? a) No b) Yes, for senior supervisors c) Yes, for all
43	Please provide any additional comments you may have.

Cybersecurity Preparedness Index – Indicators & Methodology

The Cybersecurity Preparedness Index is constructed based on 15 survey questions most reflective of a jurisdiction's cybersecurity preparedness. Based on expert judgement, each question is assigned a score between 5 (most prepared) and 0 (worst prepared). The Cyber Preparedness Index is the weighted average of the individual scores where five out of the 15 questions are considered baseline requirements and are given a weight of 10 percent and the remaining questions are assigned a weight of 5 percent. Online Annex Table 3.7.3. provides an overview of the selected questions, assigned points, and weights.

Online Annex Table 3.7.3 Construction of the Cyber Preparedness Index

Relevant Question	Weight (%)	Scoring formula	Score
1. Does your jurisdiction have a national cyber strategy, which includes the financial sector?	5	No.	0
		No, we do not have a national cyber strategy, although there are ongoing discussions on whether we should develop such a strategy.	0
		No, but the government is developing a strategy that is expected to be finalized in the next 12 months (without active involvement of the central bank / supervisors).	1
		No but we, as the central bank or supervisory agency, are currently working on a government-driven national cyber strategy, that is expected to be endorsed in the next 12 months.	2
		Yes, we have a national cyber strategy, which includes the financial sector.	5
2. Does your central bank or supervisory agency have a cyber strategy for the financial sector?	5	No.	0
		No, but we are currently developing one and expect to publish it within the next 12 months.	1
		Yes, however, it is separate and not connected to the national cyber strategy.	3
		Yes, and it is integrated into the national cyber strategy.	5
3. Does your jurisdiction have a dedicated and published cybersecurity or technology risk management regulation for the financial sector?	10	No.	0
		No, we do not have a dedicated cybersecurity or technology risk management regulation but include this risk area as part of our operational or risk management regulation.	2
		No, but we are currently developing a cybersecurity/technology risk management regulation, which will be published in 12 months.	3
		Yes, we have a dedicated cybersecurity/technology risk management regulation, which has been published.	5
4. Does your jurisdiction have a dedicated and published data privacy regulation?	5	No.	0
		No, but we are currently developing one, which will be published in 12 months.	2
		Yes.	5
5. How is the supervisory architecture organized within your jurisdiction?	10	We do not take support from the IT Department and ICT / cyber risk work is handled by generalists in an ad-hoc manner.	1
		We do not have a specialized Cyber Risk Unit as of now, but we are planning to have one soon.	2
		We leverage the skill set of our IT department to conduct ICT / cyber examinations, but these are coordinated by the Supervision Department.	3
		We have a specialized Cyber Risk Unit outside the Supervision Department.	4
		We have a specialized Cyber Risk Unit as part of the Supervision Department.	5
6. What are the methods deployed for onsite supervision of cyber risk?	10	We do not conduct onsite examinations. We do not have the legal powers to mandate external audits or forensic investigations.	0
		We require an external audit of cyber preparedness of banks/FMIs on a yearly basis.	
		We have limited capacity to conduct onsite examinations.	2
		We conduct predominantly thematic reviews. Full scope examinations are rare, but we do limited scope examinations at times. We have legal powers to mandate external audits or forensic investigations.	3
		We conduct onsite supervision (full scope or limited scope examination). Thematic reviews are generally not used but we have legal powers to mandate external audits or forensic investigations.	4
		We have a full range of approaches (full scope examination, limited scope examination, short visits and thematic reviews), as well as the legal powers to mandate external audits and forensic investigations.	5
7. What are the arrangements for offsite supervision of cyber risk?	5	At this juncture we do not have any plan to set up an offsite function for ICT / cyber.	0
		We do not have a dedicated offsite function, but we have the capability to collect ad-hoc information at a short notice.	1
		We have just established an offsite function and currently collect very limited information. We plan to strengthen the offsite function significantly in the coming year.	2
		We have a separate offsite function which collects data, which we analyze regularly.	4

		We collect a full range of offsite information that pertains to ICT / cyber. We carry out analysis of such data with a focus to identify material risks faced by the individual entity as well as the system as a whole, and we provide key inputs to the onsite team.	5	
8. Do you have powers to conduct an onsite inspection of third-party providers, if necessary?	5	Unclear	0	
		No	0	
		Yes	5	
9. How do you deal with cybersecurity incidents occurring at supervised institutions? (select all that apply)	5	We have not established the process yet.	0	
		On-site direction and control of response and recovery activities.	2	
		On-site involvement in response and recovery without taking control (i.e., advisory role).	3	
		Off-site monitoring the response and recovery activities of the institution.	4	
		Analyzing mandatory reporting of cyber incidents.	5	
10. Do you have a cyber incident reporting regime in place?	10	No	0	
		No, we don't have a dedicated and specific cyber incident reporting regime in place, but financial institutions are required to report incidents as part of their operational risk requirements.	2	
		Yes, we have a dedicated cyber incident reporting regime and financial institutions are required to report incidents by law or regulation.	5	
11. What is your approach to cybersecurity testing and exercises? (Such as penetration tests, red teaming, and effectiveness of cyber incident response and crisis management exercises.)	10	There is a mandatory cybersecurity testing regime that is actively managed by the authorities.	5	
		Tests and exercises are required and there is further guidance (e.g., on scope, coverage, periodicity, or methods).	4	
		Tests and exercises are required but there is no further guidance.	3	
		Tests and exercises are encouraged but currently not required.	1	
12. What are the arrangements for dealing with cyber incidents with the help of law enforcement authorities?	5	There are no specialized cyber-related law enforcement arrangements in place.	0	
		Law enforcement authorities have specialized cyber units and are responsible for combatting, preventing, disrupting, investigating and prosecuting cybercrime and cyber criminals. The law enforcement authorities do not have a close working relationship with the central bank and financial entities.	3	
		Law enforcement authorities have specialized cyber units and are responsible for combatting, preventing, disrupting, investigating and prosecuting cybercrime and cyber criminals. The law enforcement authorities have a close working relationship with the central bank and financial entities.	5	
13. What is the approach to strengthening cyber risk supervisory capacity?	5	There is a capacity development plan that is specific to cyber risk supervision.	5	
		There is a general capacity development plan that is implicitly applicable to cyber risk supervision as well.	3	
		There is no formalized approach yet; decisions are made as needs arise.	0	
14. What approaches are used to raise cybersecurity awareness in the financial sector and the public at large? (select all that apply)	5	(i) Co-operation with academia, (ii) Interviews, speeches, and publications, (iii) participating in, or encouraging public-private partnerships, (iv) workshops with key stakeholders		
		All 4	5	
		3 out of 4	4	
		2 out of 4	3	
		1 out of 4	2	
		None	1	
15. Do you require cyber risk supervisors to obtain and maintain relevant professional certifications?	5	No	0	
		Yes, for all.	5	
		Yes, for senior supervisors.	4	

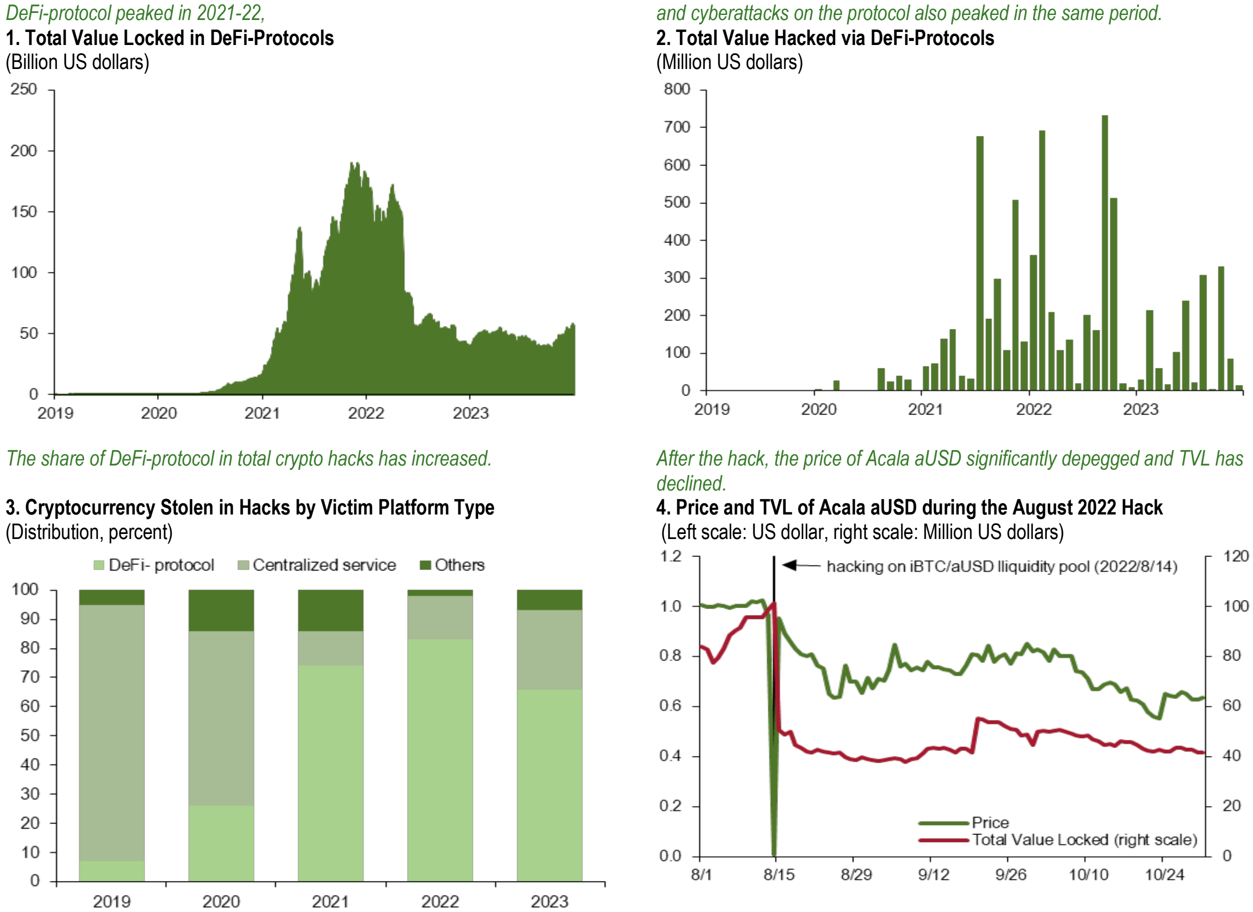
Online Annex 3.8 Cyber Incidents and Crypto Assets

Cyberattacks in DeFi-Protocols

Online Annex Figure 3.8.1 (panel 1) shows the developments in total value locked (TVL) in the DeFi-protocols—specialized autonomous programs on the blockchain network, designed to manage decentralized financial applications. The market in DeFi-protocols peaked in 2021-22 but declined in 2023, although the market is still significantly larger than in 2020. Cyberattacks on the DeFi-protocols followed these developments, with the DeFi protocols being a major target since 2021 (Online Annex Figure 3.8.1, panels 2 and 3).

Online Annex Figure 3.8.1 (panel 4) shows the developments in the price of Acala USD as well as total value locked—the overall value of crypto assets deposited in the Acala USD protocol. On August 14, 2022, hackers fraudulently minted Acala USD, such that the price plummeted and TVL significantly declined. After most of the falsely minted Acala USD was removed, the Acala USD price recovered partially, however, the TVL did not.

Online Annex Figure 3.8.1 Cyber Incidents and Crypto Assets



DeFi-protocol peaked in 2021-22,

1. Total Value Locked in DeFi-Protocols
(Billion US dollars)

and cyberattacks on the protocol also peaked in the same period.

2. Total Value Hacked via DeFi-Protocols
(Million US dollars)

The share of DeFi-protocol in total crypto hacks has increased.

3. Cryptocurrency Stolen in Hacks by Victim Platform Type
(Distribution, percent)

After the hack, the price of Acala aUSD significantly depegged and TVL has declined.

4. Price and TVL of Acala aUSD during the August 2022 Hack
(Left scale: US dollar, right scale: Million US dollars)

hacking on iBTC/aUSD lliquidity pool (2022/8/14)
1.2
1.0
0.8
0.6
0.4
0.2
0.0
120
100
80
60
40
20
0
8/1
8/15
8/29
9/12
9/26
10/10
10/24
Price
Total Value Locked (right scale)

Sources: Chainalysis; CoinCodex; DefiLlama; IMF staff calculations.
Note: 'Price' in Panel 4 represents closed price.

References

Ademann, Frank and Tamas Gaidosch. 2020. "Cybersecurity of Remote Work During the Pandemic." IMF Special Series on COVID-19

ADV Ratings. 2023. "World's Top Asset Management Firms." https://www.advratings.com/top-asset-management-firms

AM Best. 2023. "2023 Best's Rankings: World's Largest Insurance Companies - 2023 Edition". https://bestsreview.ambest.com/displaychart.aspx?Record_Code=328159&src=43

Amir, E., S. Levi, and T. Livne. 2018. "Do firms underreport information on cyber-attacks? Evidence from capital markets." Review of Accounting Studies. 23:1177-1206.

Caldara, Dario, and Matteo Iacoviello. 2022. "Measuring Geopolitical Risk." American Economic Review 112 (4, April): 1194-1225.

Dingel, Jonathan I., and Brent Neiman. 2020. "How Many Jobs Can Be Done at Home?" Journal of Public Economics 189 (September): 104235.

Financial Stability Board. 2023. "List of Global Systemically Important Banks (G-SIBs)." https://www.fsb.org/2023/11/2023-list-of-global-systemically-important-banks-g-sibs/

Häge, Frank. 2011. "Choice or Circumstance? Adjusting Measures of Foreign Policy Similarity for Chance Agreement." *Political Analysis* 19 (3): 287–305.

International Monetary Fund 2023. "Geopolitics and Financial Fragmentation: Implications for Macro-Financial Stability," Global Financial Stability Report, Chapter 3, April 2023.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M., 2021. "Risk management, firm reputation, and the impact of successful cyberattacks on target firms." Journal of Financial Economics, 139(3), pp.719-749.

P&I/Thinking Ahead Institute. 2023. "The world's largest 500 asset managers A Thinking Ahead Institute and Pensions & Investments joint study" https://www.thinkingaheadinstitute.org/content/uploads/2023/10/PI-500-2023-1.pdf

Signorino, Curtis, and Jeffery Ritter. 1999. "Tau-b or Not Tau-b: Measuring the Similarity of Foreign Policy Positions." *International Studies Quarterly* 43 (1): 115–44.

Sovereign Wealth Fund Institute. "Top 100 Asset Manager Managers by Managed AUM." https://www.swfinstitute.org/fund-manager-rankings/asset-manager