CHAPTER 3

CYBER RISK: A GROWING CONCERN FOR MACROFINANCIAL STABILITY

Chapter 3 at a Glance

- The number of cyberattacks has almost doubled since before the COVID-19 pandemic.
- Most direct reported losses from cyberattacks are small, around $0.5 million, but the risk of extreme losses—at least as large as $2.5 billion—has increased.
- The financial sector is highly exposed to cyber risks, with nearly one-fifth of all incidents affecting financial firms.
- Although cyber incidents have thus far not been systemic, severe incidents at major financial institutions could pose an acute threat to macrofinancial stability through a loss of confidence, the disruption of critical services, and because of technological and financial interconnectedness.
- Cyber legislation at the national level and better cyber-related governance arrangements at firms can help reduce the frequency of cyber incidents.
- According to an IMF survey, cybersecurity policy frameworks have generally improved in emerging market and developing economies but remain inadequate in several countries.

Policy Recommendations

- Cyber resilience of the financial sector should be strengthened by developing an adequate national cybersecurity strategy, appropriate regulatory and supervisory frameworks, a capable cybersecurity workforce, and domestic and international information-sharing arrangements.
- Reporting of cyber incidents by financial firms to supervisory agencies should be strengthened to allow for more effective monitoring of cyber risks.
- Supervisors should hold board members responsible for managing the cybersecurity of financial firms and promoting a conducive risk culture, cyber hygiene, and cyber training and awareness.
- Financial firms should develop and test response and recovery procedures to remain operational in the face of cyber incidents. National authorities should also develop effective response protocols and crisis management frameworks to deal with systemic cyber crises.

Introduction

Cyber-related incidents have become much more frequent over the past two decades, and especially since 2020.[1] In particular, the number of cyber incidents with a malicious intent ("cyberattacks")—such as cyber extortions or malicious data breaches—have almost doubled relative to the period before the COVID-19 pandemic (Figure 3.1, panel 1).[2]

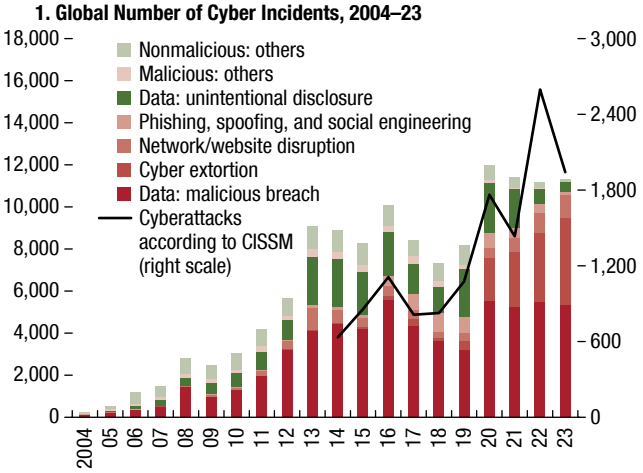
The authors of this chapter are Rafael Barbosa, Benjamin Chen, Oksana Khadarina, Tatsushi Okuda, Ravikumar Rangachary, Enyu Shao, Felix Suntheim (lead), and Tomohiro Tsuruga, under the guidance of Fabio Natalucci and Mahvash Qureshi. René M. Stulz served as an expert advisor.

[1]The cyber-related terminology in this chapter follows Financial Stability Board (2023), where "cybersecurity" is defined as the preservation of confidentiality, integrity, and availability of information through the cyber medium. "Cyber incidents" are events that adversely affect the cybersecurity of an information system or the information the system processes, stores, or transmits, thus resulting in "cyber risk." This chapter covers malicious and nonmalicious cyber incidents (excluding events related to breaches of privacy primarily directed at individuals, such as unauthorized data collection and unauthorized contact or disclosure) but focuses specifically on malicious incidents in some of the analytical exercises. Malicious events (cyberattacks) include cyber extortion, malicious data breaches, network and website disruption, phishing, spoofing, social engineering, skimming, and physical tampering. See Online Annex 3.1.

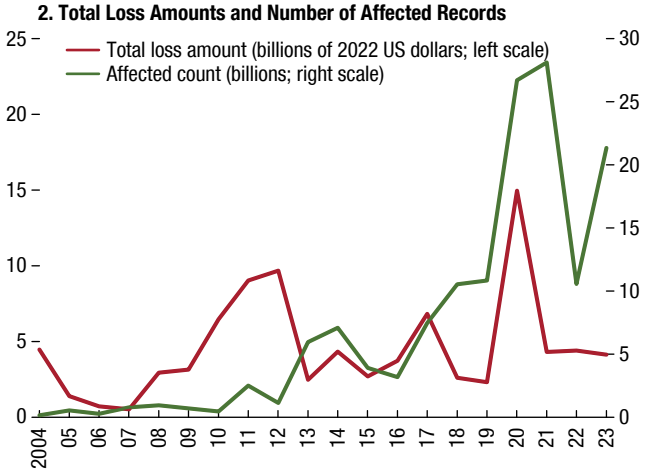
[2]The rise in cyber incidents over time could partly be attributed to improved reporting by firms, but the total number of cyber incidents and losses may still be underestimated for several reasons. These include a lag in reporting of incidents, firms' concerns about their reputation, and lack of formal requirements for firms to report cyber incidents in many countries, particularly in emerging market and developing economies.

Figure 3.1. Cyber Risks Are Increasing

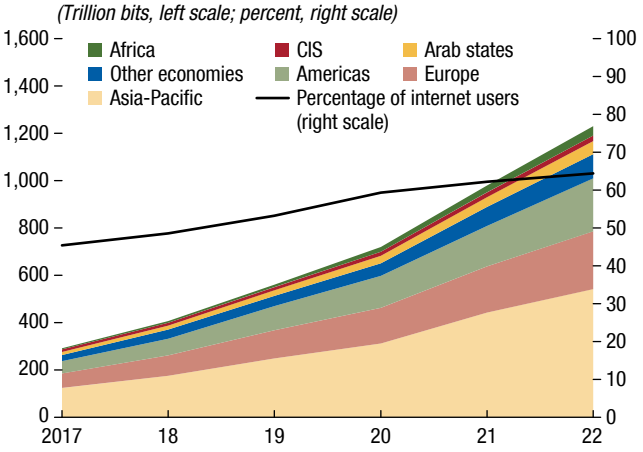
The number of cyber incidents, especially of a malicious nature, has increased sharply over the past two decades ...



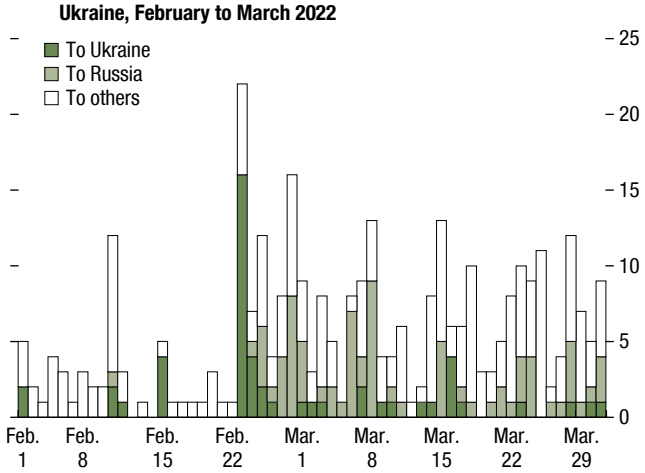
... resulting in billions of affected records and large direct reported losses.



Growing digital connectivity has likely contributed to the growth in cyber incidents.



The number of cyberattacks has surged in the wake of Russia's invasion of Ukraine in February 2022.



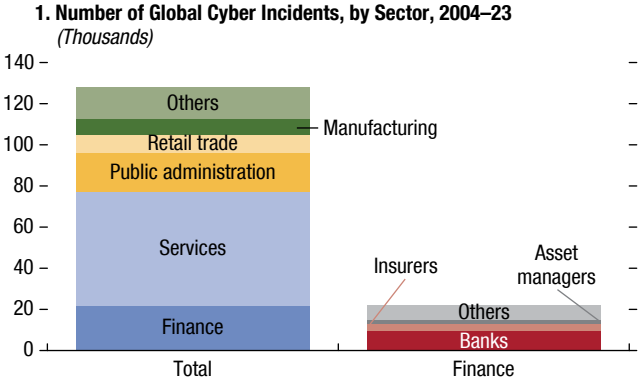
Sources: Advisen Cyber Loss Data; CISSM (Harry and Gallagher 2018); International Telecommunication Union publication; and IMF staff calculations.
Note: Panels 1 and 2 show data from Advisen (excluding events classified as "unauthorized data collection" and "unauthorized contact or disclosure"), as of February 22, 2024, using Advisen's classification of cyber incidents (see Online Annex 3.1). In panel 1, the black line shows data on cyberattacks from the CISSM. In panel 2, loss amounts are deflated using the US GDP deflator (2022 = 100). "Affected count" is the total accumulated number of parties with data breached or stolen, or devices compromised, depending on the type of event. Advisen covers a larger number of cyber incidents than CISSM, including nonmalicious incidents. Delayed reporting may lead to the underestimation of cyber events and related losses in more recent periods. CIS = Commonwealth of Independent States; CISSM = Center for International and Security Studies at Maryland.

Cyber incidents can impose substantial costs on firms. Since 2020, the aggregated reported direct losses from cyber incidents have amounted to almost $28 billion (in real terms), with billions of records stolen or compromised (Figure 3.1, panel 2). Total direct and indirect costs of these incidents, however, are most likely substantially higher (Kamiya and others 2021). Estimates range from 1 to 10 percent of global GDP (Center for Strategic and International Studies 2020; Statista 2022).[3]

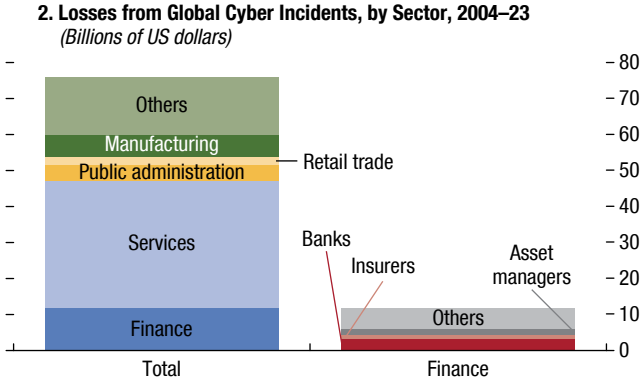
[3]Direct losses include, for example, the amount spent to remedy damages, fines and penalties, the extortion amount, or the loss of business income from operational disruptions. Indirect losses include reputational damages, declines in future business, increased cybersecurity investments, and lower productivity.

Figure 3.2. The Financial Sector Is Highly Exposed to Cyber Risk

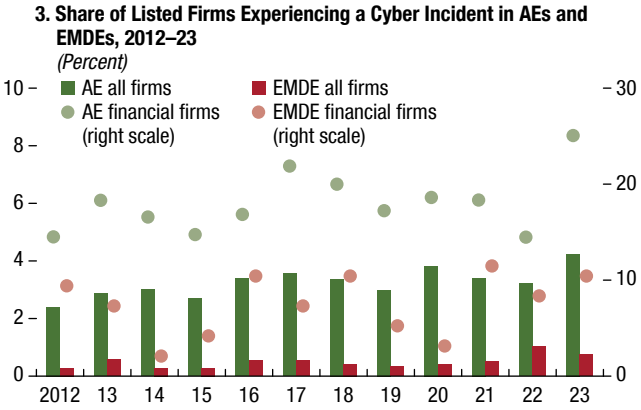
Financial institutions, especially banks, are vulnerable to cyber incidents ...



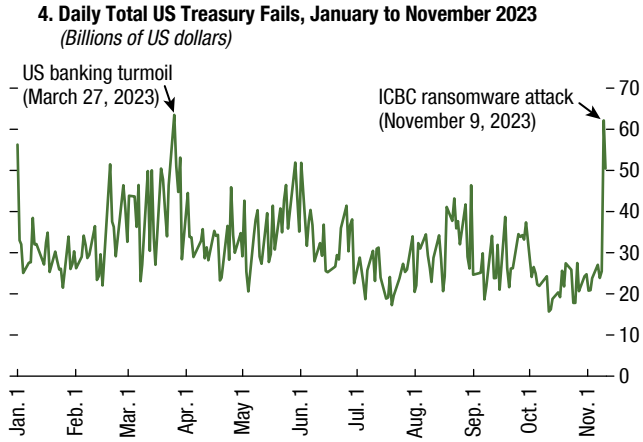
... and have experienced notable direct losses from cyber incidents.



Entities in AEs have been the most exposed, but cyber risk is also a concern in EMDEs.



A recent cyberattack on the ICBC prevented it from clearing trades, leading to disruptions in the US Treasury market.



Sources: Advisen Cyber Loss Data; Depository Trust and Clearing Corporation; and IMF staff calculations.
Note: Panels 1 and 2 are based on Advisen data as of February 22, 2024. Data for more recent periods may be underestimated because of delayed reporting of cyber events. Failures to deliver US Treasuries occur when either sellers fail to deliver or buyers fail to receive securities in time to settle a trade. AEs = advanced economies; EMDEs = emerging market and developing economies; ICBC = Industrial and Commercial Bank of China.

Many factors contribute to the rise in cyber incidents. Rapidly growing digital connectivity—accelerated by the COVID-19 pandemic (Jamilov, Rey, and Tahoun 2023), increasing dependency on technology, and financial innovation—is likely to be associated with a rise in cyber risks (Figure 3.1, panel 3). Geopolitical tensions may also be a contributing factor, considering the surge of cyberattacks after Russia's invasion of Ukraine in February 2022 (Figure 3.1, panel 4).[4]

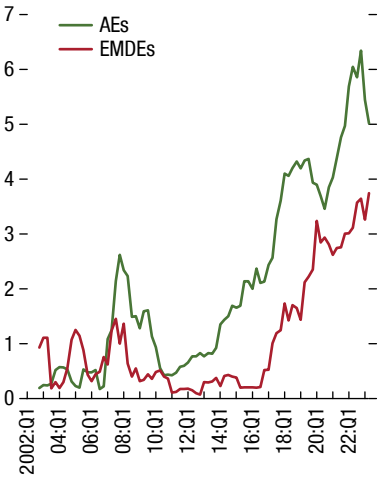
[4]Information obtained from the Center for International and Security Studies at Maryland (Harry and Gallagher 2018), as of February 2024, indicates a similar pattern for the ongoing conflict in the Middle East, where the number of cyberattacks on both Israel and Palestine increased notably at the onset of the recent conflict in October 2023.

The financial sector is highly exposed to cyber risk. Almost one-fifth of the reported cyber incidents in the past two decades have affected the financial sector, with banks being the most frequent targets followed by insurers and asset managers (Figure 3.2, panel 1). Financial firms have reported significant direct losses, totaling almost $12 billion since 2004 and $2.5 billion since 2020 (Figure 3.2, panel 2). Financial institutions in advanced economies, particularly in the United States, have been more exposed to cyber incidents than firms in emerging market and developing economies (Figure 3.2, panel 3). JPMorgan Chase, for example, the largest US bank, recently reported experiencing 45 billion cyber events per day while spending $15 billion on technology

Figure 3.3. Cyber Risks Are Receiving Increasing Attention

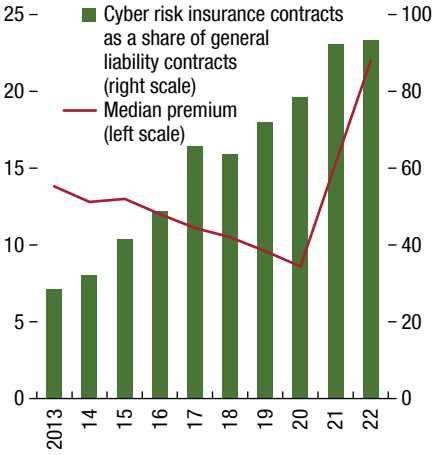
Mentions of cyber risks have increased in firms' earnings calls.

1. Cybersecurity Keywords in Firms' Earnings Calls
(Mentions per 10,000 sentences)



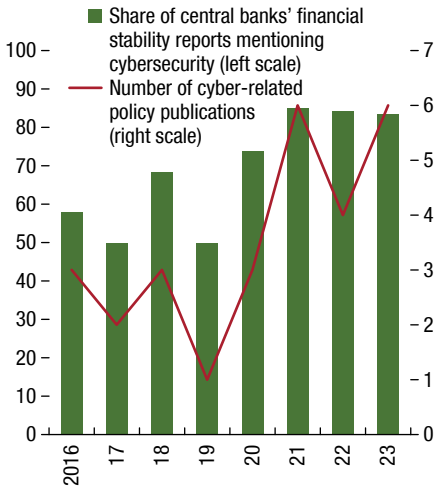
Cyber insurance coverage has risen along with insurance premiums.

2. Cyber Insurance Contracts and Median Premium for Large Companies, 2013–22
(Rate per million of insurance coverage in thousands of US dollars, left scale; percent, right scale)



Central banks and international bodies are paying growing attention to address cyber risks.

3. Coverage of Cybersecurity in Central Bank Reports and Published Cyber-Related International Policy Documents
(Percent, left scale; number, right scale)



Sources: Advisen; NL Analytics; and IMF staff calculations.
Note: Panel 1 shows the number of mentions of words related to cybersecurity (such as "cybersecurity," "cyberattack," "cyber threat," "data loss," "data integrity," "data security," "information theft," "data breach," "phishing," "malware," "ransomware") per 10,000 sentences in firms' earnings call reports. In panel 2, the green bars show the ratio of the total number of new cyber risk insurance contracts to the number of new general liability contracts for large firms (defined as those with annual revenues larger than $100 million) in a given year. The red line shows the median premium associated with the cybersecurity insurance contracts. In panel 3, the green bars show the share of financial stability reports and annual reports issued by central banks in the G20 nations that cover cyber risks, and the red line shows the number of policy publications on cybersecurity and related topics by prominent international organizations (Basel Committee on Banking Supervision, Financial Stability Board, International Association of Insurance Supervisors, International Organization of Securities Commissions, and the G7). AEs = advanced economies; EMDEs = emerging market and developing economies; G7 = Group of Seven; G20 = Group of Twenty.

every year and employing 62,000 technologists, many focused on cybersecurity.[5]

Cyber incidents are a key operational risk that could threaten financial institutions' operational resilience and adversely affect overall macrofinancial stability. A cyber incident at a financial institution or at a country's critical infrastructure could generate macrofinancial stability risks through three key channels: loss of confidence, lack of substitutes for the services rendered, and interconnectedness (Adelmann and others 2020). While cyber incidents thus far have not been systemic, ongoing rapid digital transformation and technological innovation (such as artificial intelligence) and heightened global geopolitical tensions exacerbate the risk. Recent significant cyber incidents—such as the ransomware attack on the US arm of China's largest bank, the Industrial and Commercial Bank of China, on November 8, 2023, which temporarily disrupted trades in the US Treasury market—further underscore that cyber incidents at major financial institutions could threaten financial stability (Figure 3.2, panel 4).

The private sector has become more attuned to cyber risks. Business leaders and financial sector participants consider cyber insecurity a top risk to global macrofinancial stability (Bank of Canada 2023a; Bank of England 2023; Depository Trust and Clearing Corporation 2023; World Economic Forum 2023; EY/IIF 2024). Mentions of cyber risks have surged in firms' earning call reports in the past few years, indicating that firms and analysts are paying greater attention to the issue (Figure 3.3, panel 1). Concerns about cybersecurity are also reflected in the growing share of firms taking out insurance to protect against financial losses from cyber incidents relative to general liability insurance contracts (Figure 3.3, panel 2).

[5]"Cyber events" refers here to observed activity, malicious and nonmalicious, collected from JPMorgan's technology assets. Such events can include collecting user logins and scanning for network vulnerabilities (Owen Walker, "JPMorgan Suffers Wave of Cyber Attacks as Fraudsters Get 'More Devious,'" *Financial Times*, January 17, 2024, https://www.ft.com/content/cd287352-cb3b-48d8-a85b-668713b80962).

Central banks and financial regulators are viewing cybersecurity as a material risk.[6] The European Systemic Risk Board, the Financial Stability Oversight Council in the United States, and the Bank of England's Financial Policy Committee have recognized cyber risk as a source of systemic risk (European Systemic Risk Board 2020; Financial Stability Oversight Council 2023; Bank of England, 2024b). Central banks and financial supervisors increasingly consider cyber risk in financial stability reports and supervisory stress tests (Figure 3.3, panel 3, green bars).[7] Global efforts to mitigate cyber risks in the financial sector have also accelerated, and multiple standard-setting bodies have published policy documents and guidelines to strengthen cyber resilience (Figure 3.3, panel 3, red line).[8]

[6]Cybersecurity of central banks and financial regulators is also crucial for financial stability. For example, in January 2024, the social media account of the US Securities and Exchange Commission was hacked and a fraudulent announcement regarding the approval of a bitcoin exchange-traded fund released, increasing market volatility (Krisztian Sandor, "Bitcoin Jumps, Then Dumps to $45K as Fake News about Spot Bitcoin Approval Liquidates $50M," *CoinDesk*, January 9, 2024, https://www.coindesk.com/markets/2024/01/09/bitcoin-jumps-then-dumps-to-45k-as-fake-news-about-spot-bitcoin-approval-liquidates-50m/). Overall, however, the number of incidents at such institutions has been relatively stable at 10 to 20 incidents per year (see Online Annex Figure 3.1.1, panel 3).

[7]In 2021, US Federal Reserve Chairman Jerome H. Powell remarked that "the risk that we keep our eyes on the most now is cyber risk" (*CBS News*, April 12, 2021). For references to increased cybersecurity risks, see Bank of France (2022), Bank of Mexico (2022), ECB (2022), US Department of the Treasury (2022), and Bank of Canada (2023b). In 2022, the Bank of England launched cyber stress tests as a complementary exercise to its operational resilience policy, and in March 2024 its Financial Policy Committee published a macroprudential approach to operational resilience which considered cyber risks (Bank of England 2024a). The European Central Bank plans to conduct a thematic stress test on banks' cyber resilience in 2024.

[8]The role of standard-setting bodies has gained momentum with the Basel Committee on Banking Supervision (2021) principles for operational resilience, which assume that cyber incidents will occur and that the financial sector needs the capacity to deliver critical business services during disruptions. Enhancing cyber and operational resilience is also a key element of the Financial Stability Board, which has focused on promoting convergence in cyber incident reporting, effective practices for cyber incident response and recovery, maintaining the cyber lexicon, as well as current work to design a format for incident reporting exchange (FIRE). Moreover, the Financial Stability Board published a toolkit to enhance third-party risk management and oversight for financial authorities, financial institutions, and service providers (FSB 2023). In addition, the Committee on Payments and Market Infrastructures and IOSCO (2016) issued guidance on cyber resilience to help financial market infrastructures strengthen cybersecurity; IOSCO (2021) outsourcing principles cover information security, business resilience, continuity, and disaster recovery; the International Association of Insurance Supervisors followed up a 2016 report on cyber risk with a 2023 report on operational resilience; and the G7 cyber expert group has issued several papers that help financial sector entities better understand cybersecurity topics (2016, 2017, 2018, 2020, 2022a, 2022b).

Against this backdrop, the chapter assesses the potential financial stability implications of cyber risks and discusses policy options to mitigate such risks. The chapter begins by presenting a simple conceptual framework on the potential channels through which cyber risks can disrupt macrofinancial stability. It then empirically examines three key questions. First, how large are firm-level losses from cyber incidents? Second, what factors explain the occurrence of cyber incidents? Third, how vulnerable is the financial sector to cyber risk? To address these questions, the chapter relies on various data sources, including a comprehensive firm-level data set on more than 170,000 cyber events reported by approximately 90,000 companies globally.[9] Because private incentives to address cyber risks may differ from the socially optimal level of cybersecurity, public intervention may be necessary (Kopp, Kaffenberger, and Wilson 2017; Kashyap and Wetherilt 2019). Through a survey, the chapter offers insights into the preparedness of central banks, financial regulators, and financial supervisors, particularly in emerging market and developing economies. The chapter then discusses policy options to strengthen the resilience of the financial system to systemic cyber risks.[10]

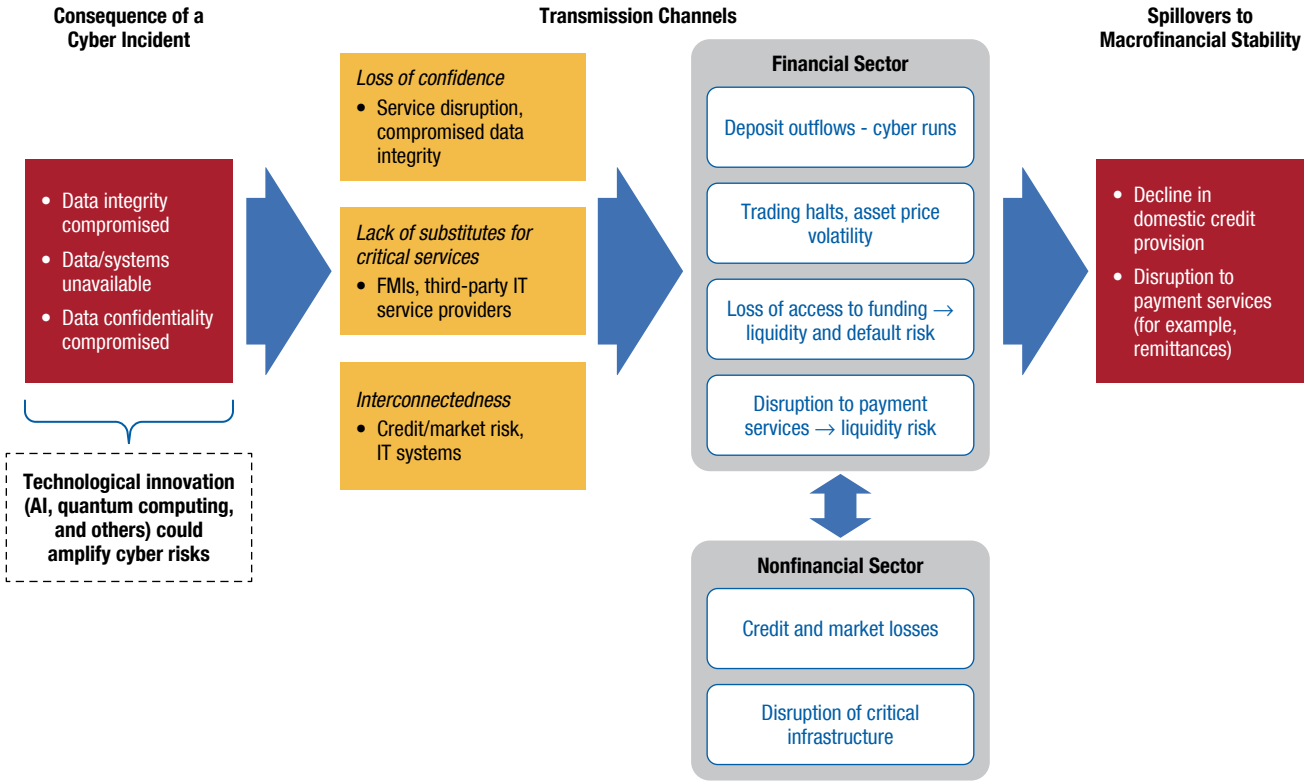
Transmission of Cyber Risks to Macrofinancial Stability

A cyber incident at a financial institution could threaten macrofinancial stability through three key

[9]Advisen Cyber Loss Data cover 40 advanced and 125 emerging market countries. This data set is compiled from reliable and publicly verifiable sources (news media, governmental and regulatory sources, state data breach notification sites, and third-party vendors). Details on the data used for the analyses are provided in Online Annex 3.1.

[10]The chapter contributes to an emerging literature on the effect of cyber incidents on firms and financial stability: A few studies have assessed the effect of cyberattacks on firm-level stock returns and accounting performance by relying on event studies (Amir, Levi, and Livne 2018) or textual analysis to capture cybersecurity risk for a cross-section of firms (Florackis and others 2023; Jamilov, Rey, and Tahoun 2023). Aldasoro and others (2022) concentrate on the drivers of losses from cyberattacks for US firms, whereas Crosignani, Macchiavelli, and Silva (2023, p. 437) show that a "supply chain attack" can cause a systemic shock. Focusing on the financial sector, Duffie and Younger (2019) show the possibility of cyberattacks leading to bank runs resulting from withdrawal of wholesale depositors. Eisenbach, Kovner, and Lee (2022) use transaction data from Fedwire to conduct a scenario analysis on the spillover effects of cyberattacks on the largest US banks. This chapter extends the literature in several dimensions—for example, by considering a larger set of countries and by examining the role of a potentially wider set of firm- and country-level characteristics in explaining the occurrence of cyber incidents, including governance and geopolitical risk. It also assesses the exposure of financial institutions to cybersecurity risks, including the likelihood of cyber runs, through different types of analyses.

Figure 3.4. Cybersecurity and Macrofinancial Stability: Channels of Transmission



Sources: Adelmann and others 2020; and IMF staff.
Note: AI = artificial intelligence; FMIs = financial market infrastructures; IT = information technology.

channels (Figure 3.4). First, a cyber incident, such as a data breach, may lead to a *loss of confidence* in the viability of the targeted institution, raising liquidity risks through, for example, deposit withdrawals or runs on banks—"cyber runs" (Duffie and Younger 2019). Such liquidity risks could result in solvency issues and possibly spill over to related parties in the financial system. Second, risks to financial stability could materialize quickly if a cyber incident were to affect a key institution or financial market infrastructure that is not easily *substitutable*. For example, a ransomware attack on major bank that participates in payment systems, the failure of key cloud service providers, hacking of a central bank, or disruption of key hubs in the financial system (such as electronic trading systems or clearing houses) could all cascade rapidly and undermine financial stability (Healey and others 2018). Third, *interconnectedness* of an institution through technological linkages (such as multiple firms using the same software) or financial linkages (such as the interbank market and settlement systems or common asset holdings) could propagate the effect of a cyber incident across the financial system (Eisenbach, Kovner, and Lee 2022). Major cyber incidents could thus adversely affect macroeconomic outcomes, for example, through a decline in the provision of credit or a disruption of payment systems.

Financial stability could also be undermined from cyber incidents at nonfinancial institutions. For example, a cyberattack on critical infrastructure (such as electricity grids) could make it difficult for financial institutions to operate normally, with the effects spilling over to the macroeconomy (Figure 3.4). Severe cyber incidents at systemic nonfinancial institutions could also raise credit or liquidity risks for financial institutions. These effects could be amplified given the potential increase in cyber risk during adverse financial conditions (Eisenbach, Kovner, and Lee 2023). Cyber incidents at public institutions could similarly disrupt government functioning. For example, an attack could

disrupt the management of government debt, adversely affecting the financial sector directly or indirectly through the rise in sovereign risk premia (April 2022 *Global Financial Stability Report*).

Emerging technologies and innovation in financial services could exacerbate cyber risks. Although advances in artificial intelligence (AI) could help improve the detection of risk and fraud, for example, by observing anomalous behavior, AI could also be exploited for malicious activities (Boukherouaa and others 2021).[11] Most notably, through generative AI (GenAI), more sophisticated phishing messages or deepfakes could be used for identity theft or fraud (Boukherouaa and Shabsigh 2023).[12] For example, in January 2024, scammers tricked employees of a multinational firm into transferring HK$200 million (US $26 million) by creating a group video call using deepfake technology.[13] In addition, AI exposes firms to the risk of data set leakages, for example, of data used to train AI algorithms or of data analyzed by third-party AI providers.[14] Looking ahead, the advent of quantum computing and its potential ability to quickly break encryption algorithms used in financial systems could also magnify losses from cyberattacks (Sedik and others 2021; Office of the President of the United States 2022).

Losses to Firms from Cyber Incidents

Direct losses reported by firms from cyber incidents have thus far been generally modest but could become very large. Based on available data, the median reported direct loss to a firm from all cyber incidents has been about $0.4 million, and three-fourths of the reported losses are below $2.8 million (Figure 3.5, panel 1). Although losses from malicious incidents have been more than five times as large as those from nonmalicious incidents, at around $0.5 million, the magnitude of losses in absolute terms has been generally modest as well. For example, most cyber extortions, such as ransomware attacks, or malicious data breaches have resulted in losses of up to $12 million. The distribution is, however, heavily skewed, with some incidents imposing losses of hundreds of millions of US dollars (Figure 3.5, panel 2). Such extreme losses could result in liquidity problems for firms and even jeopardize their solvency.[15]

The risk of extreme losses caused by cyber incidents has been increasing. Because large losses from cyber incidents are rare, accurately quantifying their probability is challenging. To address this issue, this chapter estimates a generalized extreme value distribution—an approach often used in engineering to approximate the distribution of extreme outcomes of random experiments that are highly skewed.[16] The results show that the median maximum loss in a country in a given year, or in other words, the maximum loss expected to occur in most years, has more than doubled since 2017 to $141 million in 2021, equivalent to about 50 percent of the average firm's operating income (Figure 3.5, panel 3). The analysis also suggests that once every 10 years, a cyber incident is expected to result in a $2.5 billion loss, about 800 percent of the average firm's operating income, potentially threatening the liquidity and solvency of the affected firm. Looking specifically at financial firms, the estimated maximum losses in a year are comparable—about $152 million in a median year and up to $2.2 billion once every 10 years (Figure 3.5, panel 4).

The reported direct losses of firms may not fully capture the total economic costs of cyber incidents. Firms typically do not report indirect losses from cyber incidents—such as lost business, reputational damage, or investments in cybersecurity—because these losses could be difficult to capture or may unfold over time. However, overall losses from cyber incidents (that is, both direct and indirect losses) can be estimated using the stock price reaction to

[11]AI systems could also be vulnerable to special types of attacks, such as data poisoning attacks whereby training data sets are manipulated so that algorithms incorrectly "learn" to classify or recognize information.

[12]In a survey of senior cybersecurity experts at large US companies, 46 percent expect GenAI to make organizations more vulnerable to attacks and 85 percent believe that recent attacks have been powered by GenAI (Deep Instinct 2023).

[13]Jeanny Yu, "Deepfake Video Call Scams Global Firm out of $26 Million: SCMP," *Bloomberg*, February 3, 2024, https://www.bloomberg.com/news/articles/2024-02-04/deepfake-video-call-scams-global-firm-out-of-26-million-scmp.

[14]As of June 2023, there were seven recorded instances in Advisen related to AI companies losing data after a cyber incident.

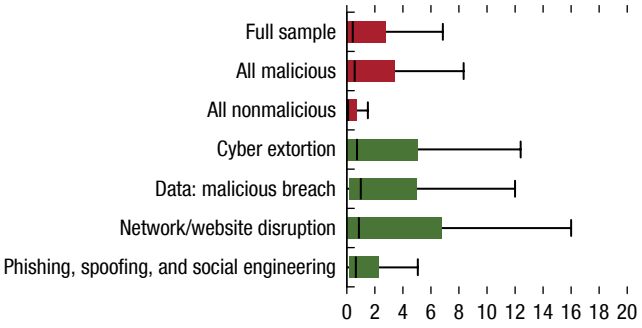
[15]For example, in 2019, Moody's lowered the credit rating outlook of Equifax, a credit reporting agency, from "stable" to "negative" after a large breach of consumer data in 2017.

[16]The generalized extreme value distribution is estimated here using data of losses caused by cyber incidents from 2012 to 2021 while controlling for country characteristics such as size (that is, GDP) and information technology infrastructure (for details, see Online Annex 3.2). Because the sample of the analysis includes only countries with more than 10 incidents per year, the results should be interpreted as the extreme loss for such countries conditional on the occurrence of cyber incidents.

Figure 3.5. Reported Direct Losses Resulting from Cyber Incidents

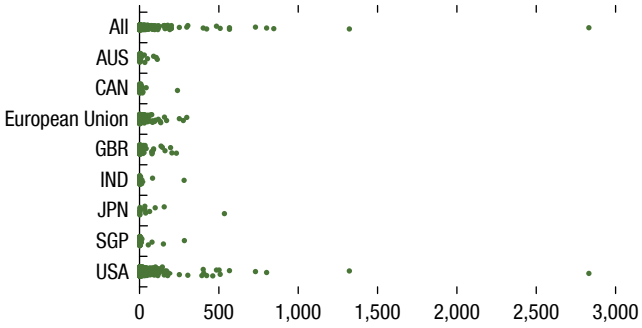
Median reported direct losses of cyber incidents to firms are modest, at about $0.4 million ...

1. Distribution of Direct Firm Losses, by Incident Type, 2012–23
(Millions of US dollars)



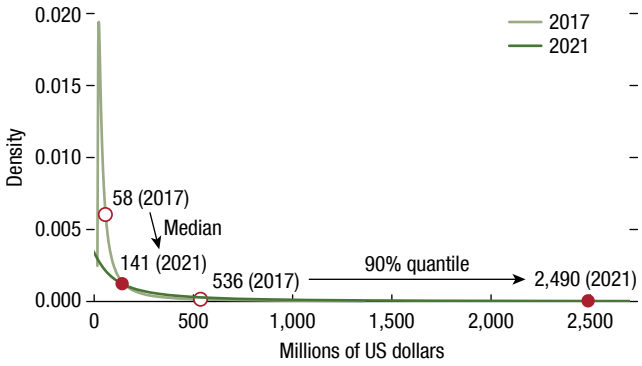
... however, very large losses can occur.

2. Distribution of Direct Losses, by Country or Group, 2012–23
(Millions of US dollars)



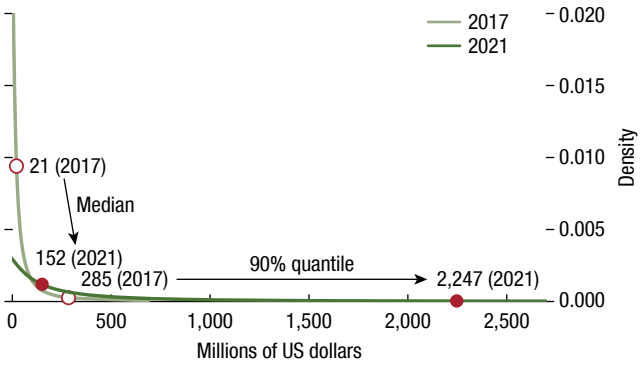
The probability of a firm experiencing an extreme loss of $2.5 billion as a result of a cyber incident is about once every 10 years ...

3. Estimated Distribution of Maximum Annual Loss, All Firms



... and, for financial firms, this extreme loss could be about $2.2 billion, up from about $300 million in 2017.

4. Estimated Distribution of Maximum Annual Firm Loss, Financial Firms



Sources: Advisen Cyber Loss Data; Capital IQ; and IMF staff calculations.
Note: In panel 1, boxes show the interquartile range and medians of losses greater than zero; whiskers represent the maximum losses (excluding outliers). In panel 2, the dots show losses greater than zero. In panel 2, data labels use International Organization for Standardization (ISO) country codes. Panels 3 and 4 show the estimated posterior density function of the highest loss of all firms and financial firms in a year.

cyber incidents because equity markets are forward looking and reflect market participants' assessment of firms' value (Kamiya and others 2021).[17] The analysis reveals that when controlling for market movements and other relevant factors, stock prices do not on average react strongly to cyber incidents (Figure 3.6, panel 1).[18] Stock prices do, however, seem to respond to cyberattacks. On average, firms' stock returns fall by 0.1 percentage points to 0.2 percentage points, although the effect is not statistically

[17]For example, the stock price of Facebook fell by about 3 percent in 2018 when the company announced that hackers had gained access to nearly 50 million user accounts (Deepa Seetharaman and Robert McMillan, "Facebook Finds Security Flaw Affecting Almost 50 Million Accounts," *Wall Street Journal*, September 28, 2018, https://www.wsj.com/articles/facebook-flaw-allowed-hackers-to-take-over-user-accounts-1538153947).

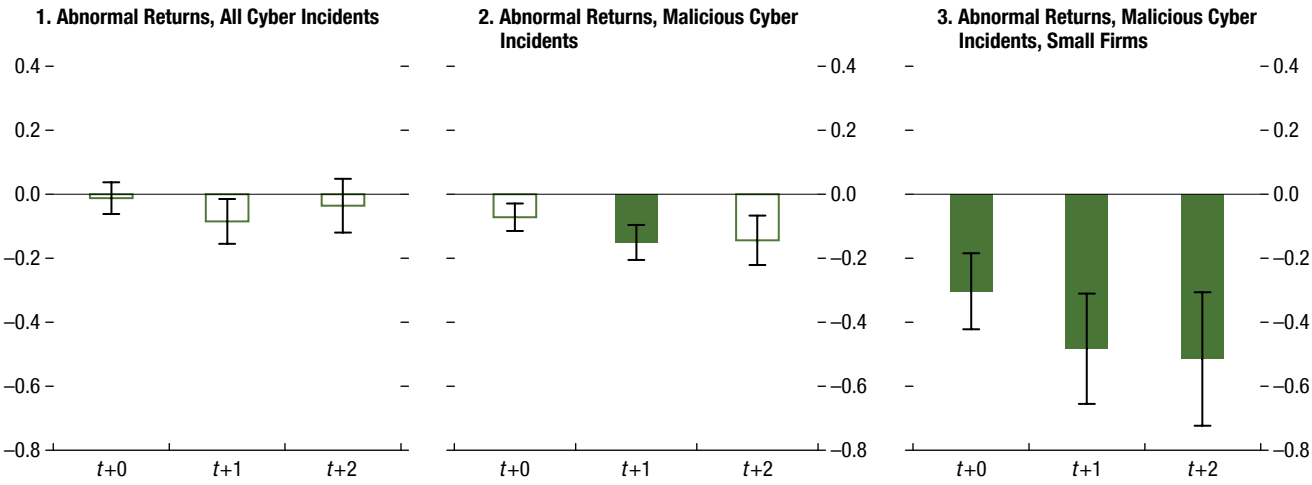
[18]The analysis relies on the assumption that equity price movements appropriately reflect losses shortly after an event is observed. The results are conditional on a cyber incident being reported, which could introduce a selection bias in the estimates. The analysis controls for overall market movements which, for major incidents, could be affected by a cyberattack on a firm. The lack of systemic cyber incidents in the past, however, suggests that cyberattacks are unlikely to affect market movements. See Online Annex 3.3 for a detailed description of the empirical methodology and robustness tests.

Figure 3.6. Total Losses from Cyber Incidents
(Percentage points)

On average, cyber incidents do not affect equity prices significantly ...

... but malicious cyber incidents are associated with a drop in equity prices of 0.1 percentage points to 0.2 percentage points ...

... and the loss is larger and more significant for smaller firms.



Sources: Advisen Cyber Loss Data; Capital IQ; and IMF staff calculations.
Note: In panels 1 and 2, results are based on event studies of 836 and 644 cyber incidents at listed firms, respectively. Small firms are firms with total assets below the 25th percentile of the sample distribution. In all panels, the whiskers represent the one-standard-deviation error band. Malicious events include cyber extortion, malicious data breach, identity fraudulent use/account access, network and website disruption, phishing, spoofing, social engineering, skimming, and physical tampering (see Online Annex 3.1). The solid bars represent significance at the 10 percent level. See Online Annex 3.3 for additional details.

strong (Figure 3.6, panel 2).[19] The losses are largest and most significant for small firms, ranging from 0.3 percent to almost 0.6 percent, suggesting that small firms have less capacity to deter and deal with the potential losses from cyberattacks (Figure 3.5, panel 3). Overall, these stock market reactions correspond to losses of up to $90 million of firms' market value and are substantially larger than firms' reported direct losses.[20]

Drivers of Cyber Incidents

Understanding the factors that contribute to the occurrence or prevention of cyber incidents is crucial for developing robust cybersecurity policies and strategies. Cyber incidents are determined by both a firm's overall exposure to cyber incidents and its ability to prevent them. For example, large and profitable firms that have an extensive digital presence and that depend heavily on informational and communication technology could be a more attractive target for a cyberattack than smaller firms with a limited digital footprint. At the same time, such firms could also have a greater capacity to invest in cybersecurity and strengthen resilience, making them less vulnerable to cyber incidents. Firms located in countries facing geopolitical tensions may also have a greater likelihood of falling victim to a cyberattack caused by threats from rival countries. Firms with mature cyber governance and firms that operate in countries with strong cyber laws, in contrast, may be more likely to prevent a cyber incident.[21]

Econometric analysis suggests that digitalization and geopolitical tensions significantly raise the

[19]The sample used in the analysis consists of firms incorporated in different countries with different reporting standards. Results are comparable across countries.

[20]At the firm-incident level in the sample, the loss in market capitalization was larger than the reported direct loss in about 90 percent of cases.

[21]Kamiya and others (2021) studied the likelihood of cyberattacks that involve the loss of personal information in a sample of US firms. They found that firms that experience such cyberattacks are larger and older; are more profitable; are less risky; have better future growth opportunities, higher leverage, and more asset intangibility; and invest less in capital expenditures and research and development.

risk of cyber incidents.[22] For example, moving from the 10th percentile on the United Nations' Telecommunication Infrastructure Index (the level of Madagascar or Malawi) to the 90th percentile (the level of Spain) raises the likelihood of a cyber incident from 0.5 percent to more than 2 percent.[23,24] This represents a notable increase, considering that the mean likelihood of experiencing a cyber incident in a given year in the sample is 1.2 percent. Countries with heightened exposure to geopolitical tensions are at a similar increased risk of experiencing a cyber incident.[25] Larger firms and those with a higher share of intangible assets—typically firms in the information technology (IT) sector—also face a notably higher probability of experiencing a cyber incident (Figure 3.7, panel 1).[26] By contrast, firms in countries with more developed cyber legislation are less likely to be targets of a cyber incident.[27]

Firms that shifted to telework during the COVID-19 pandemic were more likely to have experienced a cyber incident. Results show that cyber incidents increased more in firms that relied only moderately on telework before the pandemic but shifted to teleworking during the pandemic (Figure 3.7, panel 2). Before the pandemic, firms in sectors with a high propensity to telework were more likely to experience cyber incidents than other firms, possibly because they relied more on IT infrastructure. After the pandemic, however, the probability of such firms experiencing cyber incidents declined.[28] Firms with less telework capacity before the pandemic, conversely, were unlikely to shift to telework and were not strongly affected by cyber incidents during the pandemic.

Insufficient governance arrangements related to cybersecurity may have amplified vulnerabilities during the COVID-19 pandemic. One plausible explanation for the finding that cyber incidents increased for firms that shifted to teleworking during the pandemic but declined for those accustomed to telework before the pandemic could be that the latter had relatively stronger cybersecurity and governance arrangements, as well as a better-prepared workforce. Indeed, as shown in Figure 3.7 (panel 3), firms in sectors with a high propensity to telework before the pandemic had better governance arrangements to mitigate cyber risks. Such firms were more likely to have board members with cybersecurity expertise, to have cybersecurity and data privacy policies, and to have scored higher on an index capturing firms' ability to manage data privacy risks. The firms also further improved governance along these dimensions during the pandemic.

Firms tend to bolster their cyber defenses after an incident, indicating that managing cyber risks includes a dynamic learning process. For example, the probability of a cyberattack is 1.2 percentage points lower for firms that experienced an attack in the past two years (Figure 3.7, panel 4). Consistent with cyber governance being an important factor in preventing the occurrence of cyber incidents, there is some evidence that firms increase the number of board members with cyber expertise after a cyber incident.[29]

The Cyber Threat Landscape in the Financial Sector

The financial system is notably exposed to cyber risk. Financial firms handle large amounts of customer data and transactions, potentially making them a target of choice for cybercriminals seeking

[22]To study the drivers of cyber incidents, a probit model is estimated using global firm-level data covering 16,945 firms in 42 countries from 2014 to 2022. See Online Annex 3.4 for details.

[23]The Telecommunication Infrastructure Index is constructed by the United Nations and is a composite of four indicators: (1) estimated internet users per 100 inhabitants, (2) number of mobile subscribers per 100 inhabitants, (3) active mobile-broadband subscription, and (4) number of fixed broadband subscriptions per 100 inhabitants.

[24]The likelihood of observing a cyber incident could also be influenced by differences in reporting across countries.

[25]Geopolitical tensions are captured by the Geopolitical Risk Index (Caldara and Iacoviello 2022), which consists of a measure of adverse geopolitical events and risks based on a tally of newspaper articles.

[26]These results are consistent with those of Kamiya and others (2021).

[27]Cyber legislation is captured by the Maplecroft Cyber Legislation Index, which captures the adoption of e-commerce legislation related to e-transactions, consumer protection, data protection and privacy, and cybercrime. The index indicates whether a country has adopted legislation or has a draft law pending adoption.

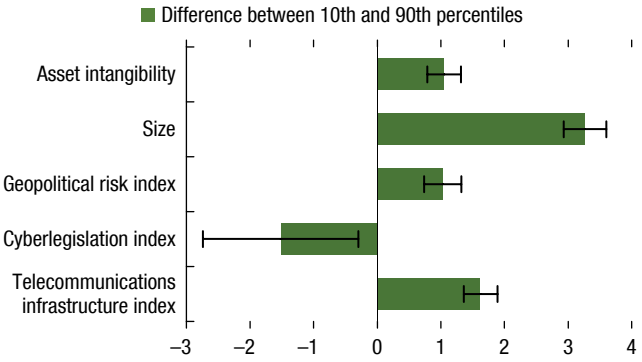
[28]The ability to telework is identified at the sectoral level based on the share of the workforce capable of working remotely before the COVID-19 pandemic (Dingel and Neiman 2020).

[29]See Online Annex 3.4 for additional details on modeling of the effect of past cyber incidents on vulnerability and robustness checks.

Figure 3.7. Drivers of Cyber Incidents

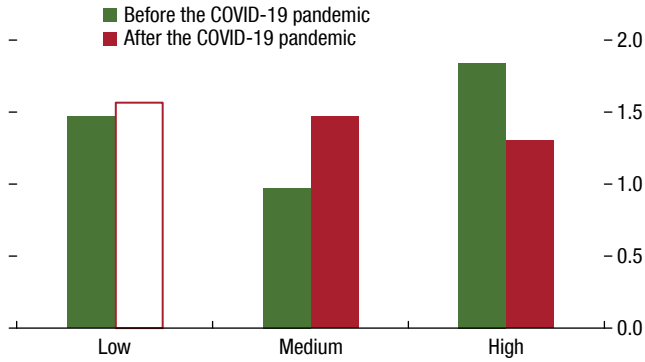
Firms in countries with more advanced technology, weaker cyber legislation, and greater exposure to geopolitical risks have a higher likelihood of experiencing a cyber incident.

1. Effect of Firm and Country Variables on the Likelihood of Cyber Incidents
(Percentage points)



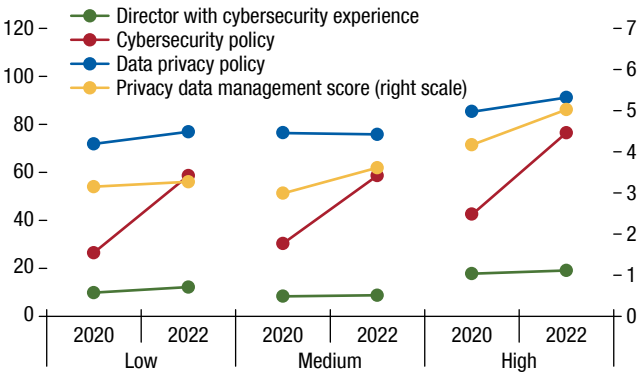
During the COVID-19 pandemic, firms in sectors that had to switch to remote working had a higher probability of experiencing a cyber incident relative to prepandemic levels ...

2. Probability of Cyber Event before and after the COVID-19 Pandemic, by Sectors' Teleworkability
(Percentage points)



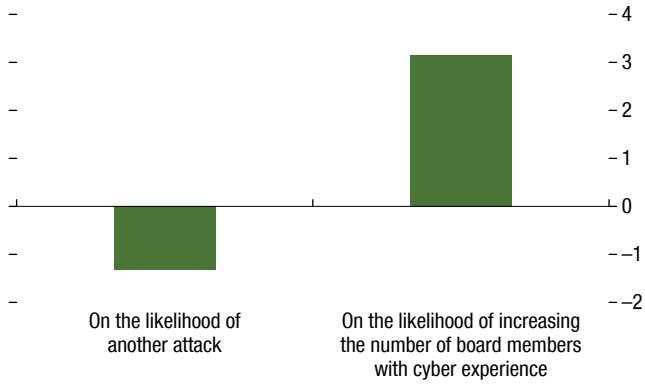
... which may, at least partly, be attributed to weaker cyber governance in place relative to the firms that already relied on telework before the pandemic.

3. Cyber Governance of Firms with Different Teleworking Capabilities
(Share of firms, left scale; score, right scale)



In general, firms seem to improve cybersecurity after cyberattacks, for example, by improving their cyber governance.

4. Effect of Cyberattacks on Future Cyber Incidents and Firms' Cyber Governance
(Percentage points)



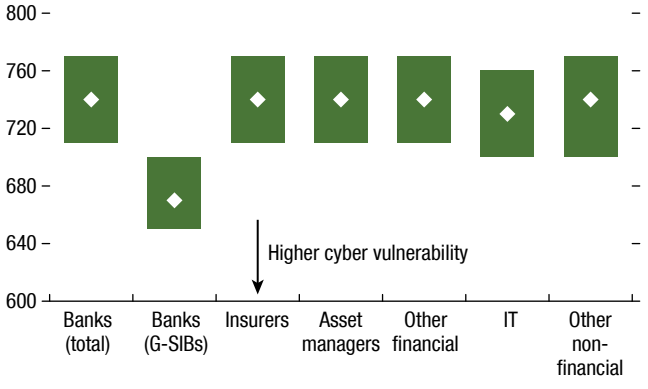
Sources: Advisen Cyber Loss Data; Caldara and Iacoviello 2022; Capital IQ; Dingel and Nieman 2020; Maplecroft; MSCI; Orbis; Refinitiv; United Nations; and IMF staff calculations.
Note: Panel 1 shows the difference in the estimated likelihood of a cyber incident when moving from the 10th percentile to the 90th percentile of the sample distribution of the specified variable while holding all other variables at mean values. Panel 2 shows the predicted probability of cyber incidents before and after the COVID-19 pandemic for firms with different levels of teleworkability, holding other variables at mean values. Panel 3 shows the share of firms with different cybersecurity-related governance mechanisms, before and after the COVID-19 pandemic, for firms with different levels of teleworkability. Teleworkability groups (low, medium, high) are based on Dingel and Nieman (2020). In panel 4, the bar on the left shows the change in likelihood of a cyberattack in a given year when a firm experienced a malicious cyber incident in the previous two years, and the bar on the right shows the change in likelihood of a firm increasing the number of board members with cyber expertise after the firm experienced a cyberattack in the previous year. The econometric models control for a range of firm-level factors and fixed effects. See Online Annex 3.4 for detailed descriptions of the econometric models and variable construction. In panel 1, the whiskers show 90 percent confidence intervals. In panels 1, 2, and 4, the solid bars represent significance at the 10 percent level.

monetary gains or disrupting economic activity. As shown in Figure 3.2 (panel 1), cyber incidents in the financial sector constitute a sizeable share of all cyber incidents, with banks facing about half of the sector's incidents. Large banks are particularly vulnerable, as suggested by ratings that capture an organization's overall cybersecurity performance—presumably because they are more often targeted, even though they may have more sophisticated cybersecurity practices in place (Figure 3.8, panel 1, and Online

Figure 3.8. Cyber Risk in the Financial Sector

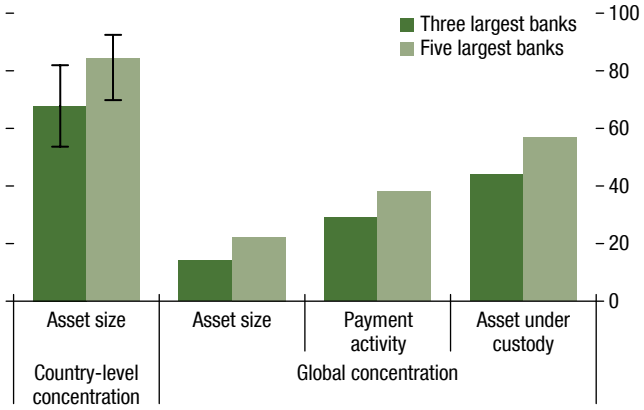
Large banks are considered particularly vulnerable to cyberattacks.

1. Distribution of Bitsight Cybersecurity Ratings, January 2024
(Index)



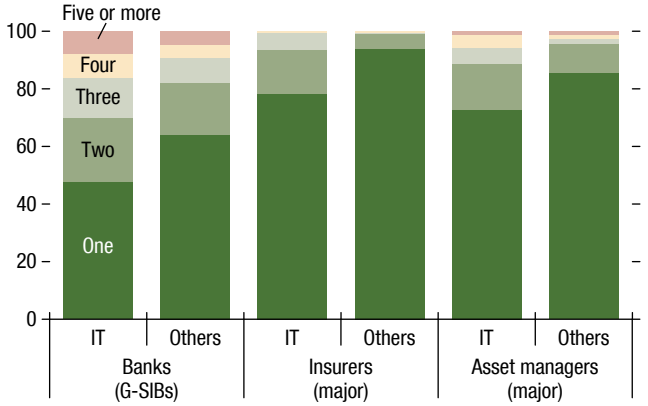
High market concentration of banks—for example, in payment and custody services—underscores the importance of cybersecurity and operational resilience.

2. Bank Concentration at the Country and Global Level, 2021
(Market share of largest banks, percent)



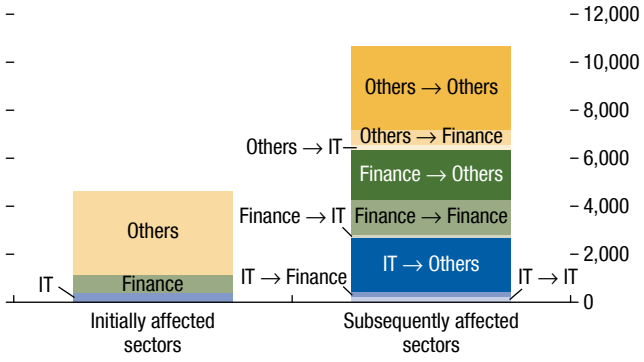
Major banks tend to share IT suppliers, raising the risk of common shocks ...

3. Percentage of Third-Party Providers Covering One or More Major Financial Firms, June 2023



... and spillovers from third-party service providers, such as in the IT sector.

4. Sectoral Distribution of the Number of Firms Affected by a Cyber Event Originating at Another Firm, 2004–23



Sources: Advisen Cyber Loss Data; Bank for International Settlements; Bitsight; FactSet; Orbis; and IMF staff calculations.
Note: In panel 1, Bitsight Cybersecurity Ratings measure an organization's security performance. Ratings range from 250 to 900, where higher values indicate lower risk. The diamonds indicate the median, and the boxes indicate the interquartile range of the ratings. In panel 2, for "country-level concentration," the bar and whiskers indicate the median and first-to-third quartile of sample countries, respectively. The "global concentration" sample covers all banks included in the 2021 G-SIB assessment. "Asset size" in country-level and global concentrations, respectively, indicate total asset and total exposures. Panel 3 indicates the proportion of third-party IT providers and other providers with one or more clients within a financial subsector (FactSet supply chain data rely on publicly available information and may be incomplete). Online Annex 3.1 indicates the definition of major financial firms. Panel 4 shows cyber events that hit one firm and affected multiple firms. The left bar shows the sectors of the firms originally affected, and the right bar shows which sectors were subsequently affected. G-SIBs = global systemically important banks; IT = information technology.

Annex 3.5).[30,31] This vulnerability underscores the critical importance of managing and mitigating cyber risk to maintain global financial stability.

Three key characteristics amplify the vulnerability of financial institutions to cyber incidents:

- First, *market concentration* of banks is high at the country and global levels when considering critical services such as payment services and custody banking (Figure 3.8, panel 2).[32] In general, banks' payment networks are a critical part of the financial system infrastructure. Cyber incidents could disrupt these networks to severely affect economic activity (Eisenbach, Kovner, and Lee 2022). Beyond banking, financial market infrastructures that include payment and securities settlement systems, central securities depositories, central counterparties, and trade repositories are typically characterized by high market concentration and lower substitutability, making a successful cyberattack on a financial market's infrastructure a major vulnerability of the financial system (Box 3.1).
- Second, operations of financial firms are becoming increasingly dependent on *common third-party IT providers* because of economies of scale and network effects. This includes adopting common software solutions, acquiring similar hardware components, and migrating to a select set of global cloud or critical service providers. As shown in Figure 3.8 (panel 3), more than 50 percent of IT providers of global systemically important banks supply their products and services to two or more global systemically important banks, implying a widespread overlap. IT providers of about 20 percent of insurers and 25 percent of asset managers, similarly, supply services to two or more institutions in their respective groups. These dependencies—which can be international (see Online Annex Figure 3.5.4)—have grown with the digitalization of the financial sector. Although third-party IT providers can benefit financial institutions, such as with improved operational resilience, they also carry risks.[33] If not properly managed, a high degree of overlap in the provision of third-party services could expose the financial system to common shocks, disrupt critical services in the event of cyber incidents, and pose significant risk to financial institutions and financial stability (Financial Stability Board 2023; US Department of the Treasury 2023). For example, cyber incidents in the IT sector have often spilled over to firms in other sectors (Figure 3.8, panel 4).[34]
- Third, a high degree of *interconnectedness* among financial institutions could exacerbate contagion and lead to a higher probability of cyber incidents having systemic implications. For example, a cyber incident that disrupts payment processing at an individual financial firm could cause a ripple effect on the liquidity and operations of other firms. Similarly, a severe cyber incident at a financial institution could undermine trust in the financial system more broadly and, in extreme cases, lead to market selloffs or runs on banks (Duffie and Younger 2019).

Cyber incidents could pose liquidity risks for banks. Depositors, particularly large institutional depositors, facing a cyber incident that disrupts financial transactions might doubt their ability to meet

[30]Bitsight Security Ratings is an example comprehensive cybersecurity assessment tool. Its ratings cover three risk vectors: (1) diligence—the steps an organization has taken to prevent attacks, their best practice implementation, and risk mitigation; (2) compromised systems—the presence of malware or unwanted software, which is evidence of security controls failing to prevent malicious or unwanted software from running within an organization; and (3) user behavior—employee activities, such as file sharing and password reuse, that can introduce malware to an organization or result in a data breach.

[31]According to Modi and others (2022), US banks' IT expenses have increased threefold from 2011 to 2021, and large banks have been increasing their IT spending at a much faster pace than small banks. He and others (2023) supports this finding, reporting that IT spending among larger US banks, normalized by asset sizes and noninterest expenses, tends to be higher than that of smaller banks. Moody's 2023 Cyber Survey (Moody's 2023) of 1,700 global firms, including financial institutions, indicates that cybersecurity spending rose by 70 percent from 2019 to 2023.

[32]Market concentration in the financial sector, including banking, has been relatively stable since the 2010s (see Online Annex 3.5).

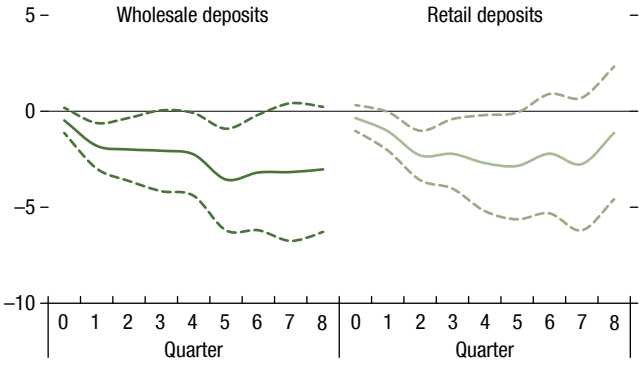
[33]Third-party IT providers to large financial firms generally have cybersecurity ratings as high as those of the financial firms themselves (see Online Annex 3.5).

[34]A ransomware attack on Trellance, a cloud IT service provider, in December 2023 caused outages at 60 US credit unions (Sean Lyngaas, "Ransomware Attack Causes Outages at 60 Credit Unions, Federal Agency Says," *CNN*, December 4, 2023, https://www.cnn.com/2023/12/01/politics/ransomware-attack-credit-unions/index.html). An update to an accounting software in 2017 was infected by the NotPetya virus, which resulted in the malware spreading to many firms, including across borders (Crosignani, Macchiavelli, and Silva 2023). Thousands of customers of a software supplied by SolarWinds were exposed to a potential cyberattack when the company updated the software in 2020 (US Government Accountability Office 2021).

Figure 3.9. Cyber Incidents and Deposit Flows

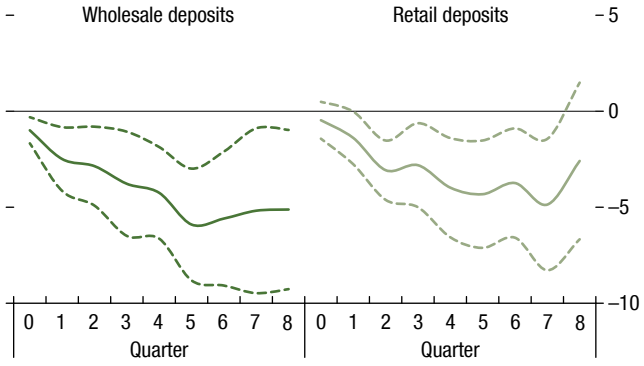
Past cyberattacks have modestly depressed deposit flows in the United States ...

1. Response of Wholesale and Retail Deposits to a Malicious Cyber Incident, Deviation from the Baseline, US Banks, 2014–22
(Percent)



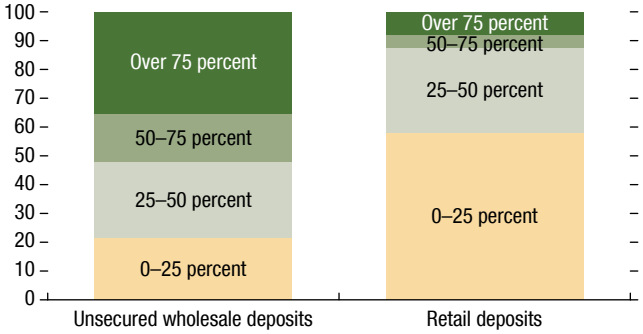
... and the effects have been more severe in smaller banks.

2. Response of Wholesale and Retail Deposits to a Malicious Cyber Incident, Deviation from the Baseline, US Smaller Banks, 2014–22
(Percent)



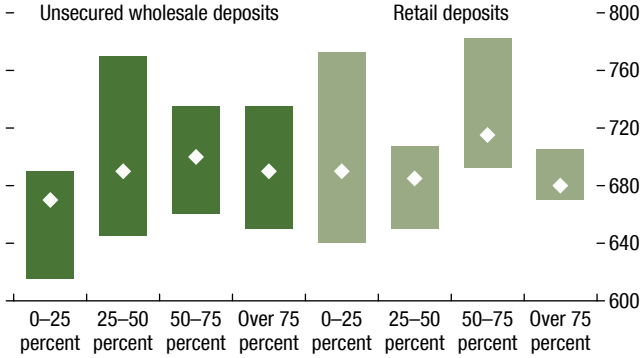
Banks that are more vulnerable to liquidity risk from outflows of wholesale and retail deposits ...

3. Distribution of Reverse Outflow Rates, September 2023
(Percent)



... also tend to have lower median cybersecurity ratings.

4. Reverse Outflow Rates and Cybersecurity Ratings
(Index)



Sources: Advisen Cyber Loss Data; Bitsight; bank disclosures; Federal Financial Institutions Examination Council; Orbis; and IMF staff calculations.
Note: In panels 1 and 2, the solid lines represent estimates of the cumulative response of banks' domestic 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). Malicious incidents include cyber extortion, malicious data breach, identity fraudulent use/account access, network and website disruption, phishing, spoofing, social engineering, and skimming and physical tampering (see Online Annex 3.1). Banks with total deposits below the two-thirds percentile are classified as small. The sample period is the first quarter of 2014 to the fourth quarter of 2022. Panels 3 and 4 cover a sample of 88 large banks included in the 2022 assessment of global systematically important banks. In panels 3 and 4, "reverse outflow rates" on the *x* axis are the outflow rates (percent) from unsecured wholesale (retail) deposits that lower bank's liquidity coverage ratio to 100 percent. In response to deposit outflows, banks are assumed to sell their high-quality liquid assets. In panel 3, the left (right) bar shows the percentage of banks with hypothetical outflow rates from unsecured wholesale (retail) deposits that would lower their liquidity coverage ratios below 100 (in intervals of 0 to 25 percent, 25 to 50 percent, 50 to 75 percent, and more than 75 percent). In panel 4, the diamonds indicate the median, and the boxes indicate the ranges of 25th to 75th percentiles of cybersecurity ratings as of January 2024. For further details, see Online Annex 3.6.

payment obligations and therefore swiftly redeem their deposits as a precautionary measure, potentially leading to cyber runs. Cyber incidents such as data breaches of depositor information could also cause potentially long-lasting reputational damage for banks, resulting in reduced net deposit flows. Although no significant cyber runs have yet occurred, as cyber incidents have had limited effect on financial transactions, empirical analysis suggests modest and somewhat persistent deposit outflows at US banks after a cyberattack (Figure 3.9, panel 1).[35] In addition, Figure 3.9, panel 2, shows that smaller banks are more susceptible to outflows after cyber incidents, suggesting that such

[35]In this exercise, in a sample of US banks over 2014–22, cumulative changes in wholesale and retail deposits are regressed on a dummy variable that takes the value of 1 if a cyber incident occurs in a bank and 0 if otherwise. To control for the effect of business cycle fluctuations and bank characteristics, period effects and bank fixed effects are included in the model. Smaller banks are defined as those with deposit holdings below the two-thirds percentile. See Online Annex 3.6 for details.

banks may not be able to regain depositor confidence quickly after a cyberattack. On average, retail and wholesale deposits at smaller banks tend to decline by about 5 percent in cumulative terms some six quarters after a cyber incident.[36]

Banks that are potentially more exposed to liquidity risk are also more vulnerable to cyber risk. To assess the possible effect of cyber incidents on large banks' liquidity positions, the deposit outflow rate is computed at which a bank's liquidity coverage ratio would drop below the 100 percent regulatory requirement (called the reverse outflow rate).[37] The results show a large variation in the reverse outflow rates for unsecured wholesale and retail deposits across a sample of 80 large global banks. When facing 25 percent outflows of wholesale (retail) deposits, the liquidity coverage ratios of about 20 (60) percent of banks would drop below 100 (Figure 3.9, panel 3).[38] Those banks that are relatively more vulnerable to liquidity risks from deposit outflows also have lower cybersecurity ratings, indicating that relatively large banks are exposed to cyber and liquidity risks (Figure 3.9, panel 4).[39]

The rapid evolution of fintech introduces additional cyber risks.[40] Fintech firms have increased the financial system's exposure to cyber threats through their digitalized operations and interconnectedness.[41] Decentralized finance—crypto-market-based financial intermediation—has grown rapidly since 2020 and cyberattacks on decentralized finance, which employs smart contracts,[42] have been common, often causing large losses (Online Annex 3.8; April 2022 *Global Financial Stability Report*). Although central bank digital currencies have not experienced any known successful cyberattacks, there could be unknown and unpredictable risks from cyberattacks because they may rely on novel technologies, such as distributed ledger technology, for which there is no widely accepted cybersecurity framework (Bank for International Settlements 2023a). Hackers have also frequently targeted crypto assets, and cyberattacks on crypto exchanges have increased. As crypto assets become more integrated into the financial system, their vulnerability may pose risks for the financial system, for example, from cyber runs on fiat-backed stablecoins (Box 3.2).

Cybersecurity Preparedness across Countries

With the global financial system facing significant and growing cyber risks, policy and governance frameworks to mitigate the risks must keep pace. This need is being recognized by standard setters and major regulators, as noted earlier (Figure 3.3, panel 3). Yet across many countries—especially in emerging market and developing economies, where cyber threats are growing in lockstep with digitalization—legal frameworks and firm-level cyber governance arrangements remain inadequate, as suggested by several indicators of cybersecurity legislation and regulation (Figure 3.10, panels 1 and 2; Online Annex Figure 3.5.1).

According to a 2021 IMF survey of central banks and supervisory authorities, cybersecurity policy frameworks in emerging market and developing economies often remain insufficient. The survey, covering 74 emerging market and developing economies, comprised 43 questions on various aspects of cybersecurity and was originally conducted in 2021 (Adrian and Ferreira 2023) with a follow-up in 2023.[43] It showed that only 47 percent of the surveyed countries had formulated a national and financial-sector-focused cybersecurity strategy (Figure 3.10, panel 3). About half had implemented dedicated

[36]"Wholesale deposits" are defined as deposits from private nondepository institutions.

[37]More specifically, the "reverse outflow rate" represents outflows from deposits with a maturity of less than 30 days (or undetermined maturity).

[38]Limited empirical evidence exists on the possible outflow rates after a severe cyber incident. On June 27, 2014, Bulgaria's largest domestic bank, First Investment Bank, experienced a 10 percent retail deposit run after false e-mails and social media rumors suggested the bank had a liquidity shortage (Bouveret 2018). Duffie and Younger (2019) consider scenarios with 50 percent and 75 percent 30-day cumulative outflows of unsecured wholesale deposits.

[39]Although banks face regulatory capital requirements that take operational risk (including cyber risk) into account, liquidity requirements are not primarily designed on the basis of stress scenarios that include cyber incidents (Duffie and Younger 2019).

[40]Fintech (financial technology) is technological innovation in financial activities (see Chapter 3 of the April 2022 *Global Financial Stability Report*).

[41]For example, open finance facilitates innovation in financial products and services by allowing financial firms to share customer data with other firms through digital channels.

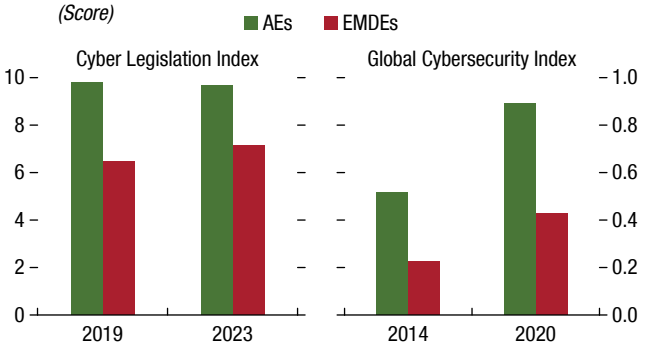
[42]Smart contracts are self-executing computer programs that automatically enforce contract terms. Because smart contracts are publicly viewable, hackers can scan them for vulnerabilities.

[43]Of the 74 countries surveyed in 2023, 37 were low-income developing countries. See Online Annex 3.7 for the list of countries and the survey questions.

Figure 3.10. Emerging Market and Developing Economies Have Gaps in Their Cybersecurity Preparedness

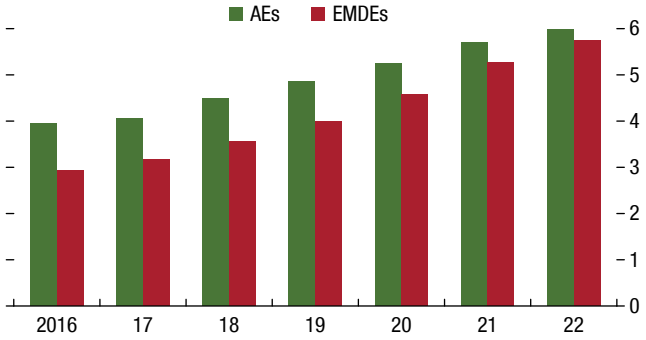
Cybersecurity-related legal frameworks in EMDEs have been improving but still lag those in AEs ...

1. Maplecroft Cyber Legislation Index and ITU Global Cybersecurity Index
(Score)



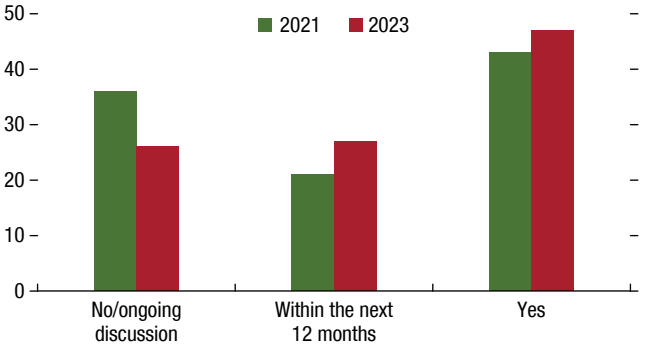
... as do firm-level cyber governance arrangements.

2. MSCI Privacy and Data Security Management Scores
(Score)



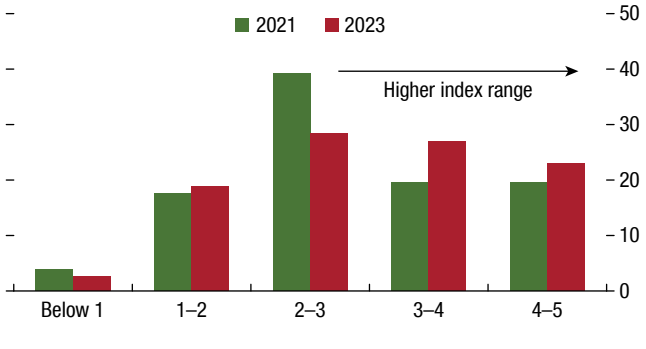
An IMF survey shows that many EMDEs lack a national cybersecurity strategy ...

3. Countries with National Cyber Strategy, IMF Survey Responses
(Percent)



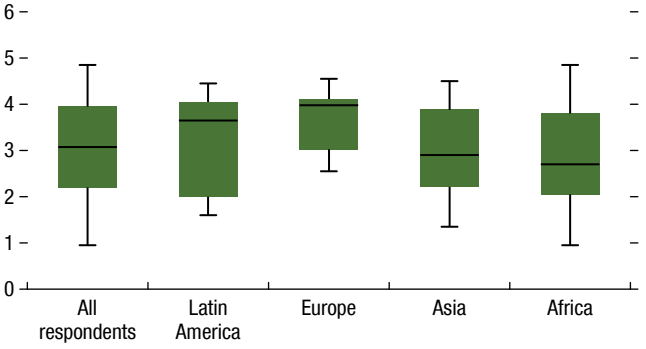
... and although cybersecurity frameworks in EMDEs have improved, they are not yet adequate.

4. Frequency Distribution of Cyber Preparedness Index Score
(Percent)



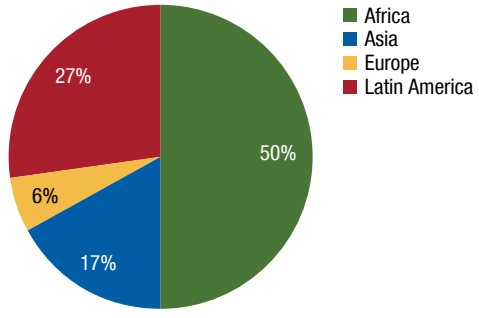
Cyber preparedness is poorest among supervisors and regulators in Asian and African countries ...

5. Cyber Preparedness Index Average, by Region, 2023
(Percent)



... making them priorities for the IMF's capacity-building efforts.

6. Cybersecurity-Related IMF Capacity-Building Activities, by Region, 2021–23
(Percent)



Sources: ITU; MSCI; Verisk Maplecroft; and IMF staff calculations.
Note: The Maplecroft Cyber Legislation Index in panel 1 ranges from 0 to 10 and captures the adoption of e-commerce legislation in e-transactions, consumer protection, data protection/privacy, and cybercrime. In panel 2, the MSCI Privacy & Data Security Management Score measures how well a company manages the risk and opportunities, with higher scores indicating better management. Panels 3 to 5 are based on an IMF survey of 74 EMDEs comprising 43 questions on various aspects of cybersecurity. In panels 4 and 5, the Cyber Preparedness Index ranges from 0 to 5 and captures the quality of cyber strategies and regulation, supervisory practices, incident reporting arrangements, approaches to cybersecurity testing, awareness building, and supervisory capacity building. See Online Annex 3.7 for the survey questions, the list of countries covered, and details on the construction of the index. In panel 6, capacity-building activities include IMF regional workshops and bilateral technical assistance missions. AEs = advanced economies; EMDEs = emerging market and developing economies; ITU = International Telecommunication Union.

cybersecurity regulations and 54 percent had adopted data privacy laws.

Analyzing the various dimensions of the survey shows that approaches to cybersecurity supervision and testing in emerging market and developing economies have improved somewhat since 2021:

- Half of the surveyed emerging market and developing economies reported that they have specialized cyber risk supervision units, and 72 percent mandate regular cyber tests and exercises, with 22 percent actively managing such tests.[44]
- Almost half of the surveyed jurisdictions have the power to examine third-party service providers—a crucial development given the increasing number of financial institutions migrating operations to the cloud.[45]
- Formal cyber risk stress tests remain less common, with 27 percent of the surveyed economies including cyber risk in their stress test programs.[46] Only 8 percent of jurisdictions had developed a cyber map that identifies the main technological and service connections between financial institutions.
- Information-sharing arrangements in the financial sector help prevent cyber threats, but only 28 percent of jurisdictions report that financial entities systematically share information and intelligence with one another. Although central banks and supervisory authorities increasingly participate in domestic industrywide information sharing, the number of countries that share data with other jurisdictions did not increase (about 50 percent). Only 49 percent of countries have cybersecurity incident reporting regimes.

The Cybersecurity Preparedness Index captures the regulatory and supervisory capacity to address cyber risks, revealing gaps among emerging market and developing economies. Based on the survey results, the Cybersecurity Preparedness Index has been created across countries to summarize the quality of cyber strategies and regulation, supervisory practices, incident reporting arrangements, approaches to cybersecurity testing, awareness building, and supervisory capacity building (Figure 3.10, panel 4). The index ranges from 0 to 5, with a score of 5 representing the highest level of cyber preparedness—comparable, for example, to the level of the United States.[47] The average score of the index across emerging market and developing economies in 2023 is 3 (slightly up from 2.8 in 2021), which indicates a moderate level of cyber preparedness. Half of the countries score below 3, and more than one-fifth score below 2, highlighting serious shortcomings in their capacity to mitigate cyber risks.

A regional breakdown of the index suggests relatively lower levels of cyber preparedness across Africa and Asia. While regulatory and supervisory capacity appears to have improved in Latin America, cyber preparedness in African and Asian countries remains, on average, relatively low (Figure 3.10, panel 5). About two-thirds of recent IMF capacity-building initiatives related to regulatory and supervisory aspects of cybersecurity have focused on these regions (Figure 3.10, panel 6).

Consistent with the survey results, IMF surveillance and capacity-building activities suggest that countries, especially among emerging market and developing economies, need to do more to address cyber risk. The IMF and World Bank Financial Sector Assessment Programs that have considered cybersecurity regulation and supervision have often found (1) gaps in national and financial sector cybersecurity strategies and coordination among stakeholders; (2) deficiencies in boards' cyber competence and effective oversight of third-party service providers; and (3) weaknesses in cybersecurity regulations and supervision, incident reporting regimes, and cyber testing requirements.[48] Lack of awareness, resources constraint, and competing priorities often hinder further progress.

[44]Regular cyber tests include vulnerability assessments, penetration testing, and red team testing (that is, threat intelligence-based testing).

[45]In the 2023 survey, 38 percent of countries noted that several or most financial institutions in their jurisdiction are migrating to the cloud, up from 27 percent in 2021.

[46]Cyber risk stress tests, an emerging practice, typically focus on testing the financial systems' resilience to cyber events. An example is testing whether contingency plans are in place to deliver critical services through disruption. These tests are also referred to as cyber resilience stress tests.

[47]See Online Annex 3.7 for a detailed explanation of the construction of the Cybersecurity Preparedness Index.

[48]The regulation and supervision of cyber risk is increasingly covered in the IMF and World Bank's Financial Sector Assessment Programs, for example, for Iceland (2022), Mexico (2022), South Africa (2022), the United Kingdom (2022), and Sweden (2023).

Conclusion and Policy Recommendations

Cyber risks pose an evolving threat to financial stability. Cyber incidents, particularly of a malicious nature, are becoming more frequent globally. The analysis in this chapter shows that losses from cyber incidents have generally been modest in the past, but they could be extreme in some cases. Although the financial sector has not yet seen a systemic cyberattack—suggesting that cybersecurity at financial firms may have been commensurate with past threat levels—the risks have increased substantially against a backdrop of growing digitalization, evolving technologies, and rising geopolitical tensions. Cyber incidents now pose an acute threat to macrofinancial stability because the sector is characterized by exposure to sensitive data, high levels of concentration, and strong interconnectedness—including with the real economy.

Private incentives to address cyber risks may differ from the socially optimal level of cybersecurity, making public intervention necessary. Firms may not fully account for the systemwide effects of cyber incidents when investing in cybersecurity—especially in the financial sector, where disruptions to critical services or a loss of confidence in the financial system can have far-reaching consequences. Firms may also underestimate risks from common vulnerabilities, for example, when using the same services or software, or lack incentives to sufficiently monitor third-party service providers. They can also be reluctant to share information on cyber incidents, for example, for reputational reasons, even though sharing such information would be desirable from a financial stability perspective to understand common vulnerabilities and prevent incidents across firms.

A cybersecurity strategy for the financial sector, accompanied by effective regulation and supervisory capacity, can help build resilience (Gaidosch and others 2019). Adequately skilled cyber risk supervision units need to be established to periodically conduct on-site assessments and collect relevant data for off-site supervision to assess the cybersecurity landscape. Mapping financial and technological connections should be carried out to identify potential systemic risks from interconnectedness and concentrations in third-party service providers (Adelmann and others 2020). Supervisors should also encourage cyber "maturity" among financial sector firms. This entails board-level access to cyber expertise, a three-lines-of-defense approach (managing risk at the business, risk management, and audit levels), cyber hygiene to improve firms' online security and maintain system health (such as antimalware and multifactor authentication), and cyber training and awareness.[49]

To effectively monitor cybersecurity, reporting of cyber incidents to supervisory agencies should be strengthened. Lack of data is a critical impediment to effective supervision and financial stability analysis as well as to firm-level risk management. Firms' reporting of cyber incidents and of the associated losses has improved in recent years, but it remains incomplete and is available with a lag (see Online Annex Figure 3.1.1, panel 1). Data collection of cyber incidents needs to be prioritized globally, and information should be shared among financial sector participants to enhance their collective preparedness.

Supervisors should require financial firms to develop and test response and recovery procedures to remain operational amid cyber incidents. Banks are subject to significant capital requirements to recover from operational risk (Afonso, Curti, and Mihov 2019), including cyber risk. Yet being able to deliver critical services during disruptions is equally important to limit potential disruptions of the financial system. To this end, firms need to identify their critical business services and ensure that tested disaster recovery plans and a crisis management framework are in place. National authorities should also develop effective response controls and crisis management frameworks to deal with systemic cyber crises.

The monitoring of cyber-related liquidity risk is warranted. Deposit outflows in the aftermath of cyberattacks have been modest in the past, and liquidity requirements on banks appear to have generally been sufficient to address them (Figure 3.9, panels 1 and 2). However, looking ahead, when assessing adequacy of liquidity under stress scenarios firms will need to consider cyberattacks and be prepared. Moreover, central bank business continuity contingency plans should factor in cyber risk, including for the provision of liquidity in a crisis.

[49]According to Microsoft (2023), the majority of cyberattacks are preventable by practicing cyber hygiene, such as enabling multifactor authentication, applying zero trust principles, using antimalware, and keeping software up to date. Training and awareness among stakeholders and a security-oriented culture can also contribute to better cybersecurity. Encryption of data helps ensure that it cannot be used when it is stolen.

Given the global nature and systemic implications of cyberattacks, cross-border coordination is crucial to mitigate cyber risks. Cyberattacks often emanate from outside a financial firm's home country and proceeds can be routed across borders, which impedes the process of holding attackers accountable and recovering the money. It is essential, therefore, to develop international protocols on cooperation to address cybersecurity issues successfully. Furthermore, reporting of cyber incidents needs to be harmonized across countries to facilitate information sharing across borders.[50]

Governments need to facilitate institutional arrangements to preserve cybersecurity. Cybersecurity laws that criminalize cyberattacks and a national cybersecurity strategy that includes identifying critical infrastructure, establishing computer incident response teams, and spreading public awareness on cyber hygiene can all contribute to enhancing cyber preparedness.

Cyber insurance could help offset cyber risks but is restricted in terms of availability and uptake.[51] Firms are increasingly relying on cyber insurance to protect against financial losses from cyber incidents (Figure 3.3, panel 2), but coverage limits remain low. About 60 percent of insurance policies in the United States have coverage limits below $1 million, and almost all have coverage below $10 million.[52] Lack of data—particularly on total losses from cyber incidents, on attacks that were attempted but did not materialize, and on key risk indicators such as investments in cybersecurity—might contribute to the restricted availability of cyber insurance.

The IMF actively helps member countries conduct cyber risk assessments and strengthen cybersecurity frameworks for the financial sector. This is mainly done through the Financial Sector Assessment Programs as well as other capacity-building initiatives such as training courses, workshops, and technical assistance missions. The IMF has also developed the Cyber Risk Supervision Toolkit comprising model regulation, a risk assessment tool, a supervisory process document, and a supervisory manual. In addition, the IMF is vital in the development of international-level cyber-related policies, contributing to efforts by standard-setting bodies such as the Basel Committee on Banking Supervision, the Financial Stability Board, and the International Organization of Securities Commissions.

[50]The Financial Stability Board (2023) has issued recommendations to achieve greater convergence in cyber incident reporting. If implemented, these recommendations should help countries establish an effective incident reporting regime that gathers required information on cyber incidents. The Financial Stability Board is also designing a format for incident reporting exchange (FIRE), which provides an approach to promote common information elements and requirements for incident reporting.

[51]The availability of insurance, particularly if it covers ransomware, could also facilitate ransom payments and thus make attacks more attractive.

[52]Insurance policy coverage limits are based on data from Advisen Client Insight.

Box 3.1. Cyber Risk for Financial Market Infrastructures

Financial market infrastructures play a critical role in the global financial system by facilitating the clearance and settlement of payments, securities, derivatives, and other financial transactions. Financial market infrastructures include payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories. Because financial market infrastructures conduct significant transaction volumes (Figure 3.1.1, panel 1), cyberattacks could affect the entire financial system.

Although major cyberattacks have not yet disrupted the operations of financial market infrastructures, payment systems have experienced outages. In 2020, a software error disrupted the payment and settlement operation of the European Central Bank's TARGET2 system for approximately 11 hours, leading to a complete failure of all payment transactions in the system. Backup systems and contingency modules were also initially unable to function. In 2021, an operational error caused nearly all US Federal Reserve Board services, such as Fedwire and FedACH, to be unavailable or significantly limited for 3 hours. In December 2023, a cyberattack disrupted the national payment system in Lesotho, preventing local banks from conducting interbank transactions in the country.

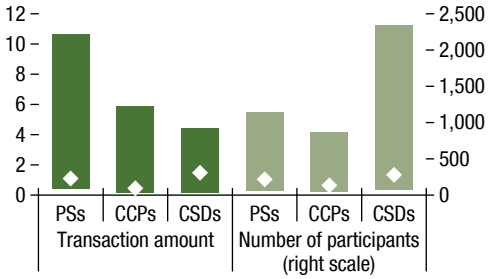
The dependence of financial market infrastructures on critical service providers, such as IT infrastructures or telecommunications services, could increase cyber risk. For example, banks and their payment systems are often attacked in the form of fraudulent payment messages passed through the SWIFT system—a messaging platform for financial transactions used by more than 11,000 financial institutions in more than 200 countries (Figure 3.1.1, panels 2 and 3). During these attacks, many of which are targeted at banks in emerging market and developing economies, hackers gain access to victims' credentials and send fraudulent payment orders, sometimes routed through advanced economy banks and central banks.

Among all SWIFT-related cyberattacks, the Bangladesh Bank heist in February 2016 caused the largest known losses, whereby hackers stole credentials from the bank and sent fraudulent transfer requests to the Federal Reserve Bank of New York that held the Bangladesh Bank's account. Although the New York Federal Reserve could block most transactions (totaling $850 million), approximately $101 million was transferred to foreign bank accounts and $81 million was later funneled through casinos, making it challenging to track the lost money. In response to such incidents, SWIFT

Figure 3.1.1. Size and Interconnectedness of Financial Market Infrastructures

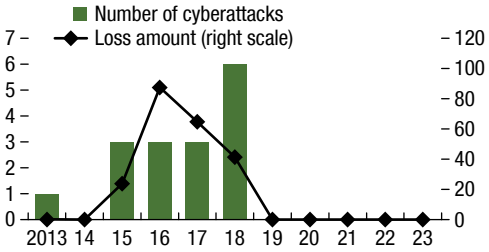
Financial market infrastructures facilitate transactions globally through connections with financial firms.

1. Transaction Amount and Number of Participants of the Top 20 Financial Market Infrastructures, 2022
(Transaction value divided by world GDP, left scale; number, right scale)



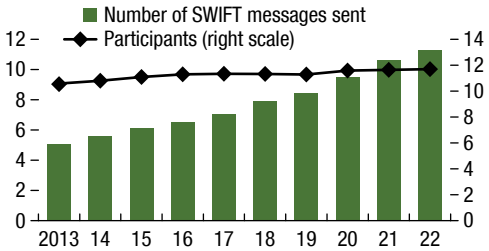
Emerging market and developing economies have experienced cyberattacks through fraudulent SWIFT messages ...

2. SWIFT-Related Cyberattacks, 2013–23
(Number, left scale; millions of US dollars, right scale)



... while activity on SWIFT has been expanding.

3. SWIFT Message Flows and Participants, 2013–22
(Billions, left scale; thousands, right scale)



Sources: Advisen Cyber Loss Data; Bank for International Settlements; and IMF staff calculations.
Note: In panel 1, diamonds indicate the median and boxes indicate the ranges of 10th to 90th percentiles. The top 20 financial market infrastructures are based on the ranking of the transaction amounts in each category. PSs includes the Continuously Linked Settlement international payments system, which provides foreign exchange settlement services. CCPs = central counterparties; CSDs = central securities depositories; PSs = payment systems.

Box 3.1 *(continued)*

established the Customer Security Controls Framework in 2016, which includes control guidelines for users to securely manage their SWIFT environment.[1] Still, in May 2018, Banco de Chile suffered a $10 million theft after cyberattacks on 9,000 computers and 500 servers obscured a fraudulent SWIFT transfer. To secure accounts, the bank disconnected workstations and suspended operations at 400 branches for two weeks.[2] Since 2019, however, SWIFT-related cyberattacks have been less successful, suggesting that the framework has been effective and highlighting the importance of coordinated efforts to improve users' preparedness.

Ensuring the cyber resilience of financial market infrastructures and strengthening their response and recovery capabilities is critical for the overall resilience of the financial system. Significant international efforts have been devoted to addressing cyber risk in financial market infrastructures, such as guidance by the Committee on Payments and Market Infrastructures and International Organization of Securities Commission (2016) on establishing and operationalizing a cyber-resilience framework. The IMF has also received several requests for capacity development and training on cyber risk of financial market infrastructures since 2022. Yet cybersecurity of some financial market infrastructures may still fall short. According to the Committee on Payments and Market Infrastructures and International Organization of Securities Commission (2022), some financial market infrastructures lack cyber response and recovery plans to meet the objective of a two-hour recovery time in the event of an extreme cyberattack scenario or cannot meet the objective at. Many financial market infrastructures, furthermore, do not conduct cyber resilience testing that meets the standards set by the guidance.[3]

[1]The Customer Security Controls Framework has three objectives: (1) "Secure the environment" by restricting internet access and protect critical systems from the general IT environment, reducing attack surface and vulnerabilities and physically securing the environment; (2) "Know and limit access" by preventing compromise of credentials, managing identities, and segregating privileges; and (3) "Detect and respond" by detecting anomalous activity in systems or transaction records and planning incident response and information sharing. To achieve these objectives, the SWIFT Customer Security Controls Framework v2024 contains 32 security controls, 25 of which are mandatory (SWIFT 2023).

[2]For details of these SWIFT-related cyberattacks, see Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions," https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

[3]A total of 37 financial market infrastructures from 29 jurisdictions voluntarily participated in the assessment. The assessment was conducted based on a self-assessment questionnaire. For details, see CPMI-IOSCO (2022).

Box 3.2. Cyber Risk and Crypto Assets

As crypto assets become more widely adopted, they are increasingly targeted by cyberattacks (Figure 3.2.1, panel 1). These attacks frequently focus on crypto asset exchanges, platforms, and hot wallets,[1] and on major crypto assets (such as bitcoin and ether). For example, in 2014, the crypto exchange Mt. Gox suffered a loss of 850,000 bitcoins because of hacks. In 2016, $60 million in ether was stolen from the DAO, a member-owned decentralized autonomous organization on the Ethereum platform. In 2021, more than $600 million was taken from the decentralized finance platform Poly Network.[2]

Crypto assets are not only vulnerable to cyberattacks but are also used in ransomware attacks, which have greatly increased since 2019 (Figure 3.2.1, panel 1). For example, in 2017, attackers using WannaCry ransomware demanded that victims pay ransom in bitcoin to unlock their encrypted files. In 2021, Colonial Pipeline paid hackers a ransom of nearly 75 bitcoins (equivalent to $4.4 million) in exchange for a decryption tool.[3]

While spillovers from cyberattacks on crypto assets to the broader financial system have been limited, crypto assets—in particular, stablecoins—raise the risk because

[1]Hot and cold wallets are the primary means of storing and exchanging crypto assets. Hot wallets are internet-enabled and online, whereas cold wallets are offline and come in the form of a physical device, such as a USB stick. The theft of crypto assets from exchanges, such as Coincheck and Zaif, in 2018 was done via hot wallets.

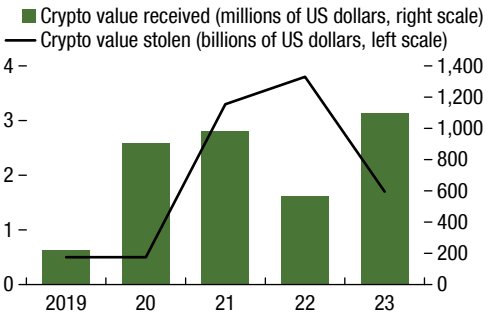
[2]For details of cyber incidents affecting Mt. Gox, DAO, and Poly Network, see Mark Memmott, "Mt. Gox Files for Bankruptcy; Nearly $500M of Bitcoins Lost," *NPR*, February 28, 2014, https://www.npr.org/sections/thetwo-way/2014/02/28/283863219/mtgox-files-for-bankruptcy-nearly-500m-of-bitcoins-lost; David Z. Morris, "CoinDesk Turns 10: 2016—How The DAO Hack Changed Ethereum and Crypto," *Consensus*, May 9, 2023, https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto/; and Eliza Gkritsi and Muyao Shen, "Cross-Chain DeFi Site Poly Network Hacked; Hundreds of Millions Potentially Lost," *Consensus*, August 10, 2021, https://www.coindesk.com/markets/2021/08/10/cross-chain-defi-site-poly-network-hacked-hundreds-of-millions-potentially-lost/.

[3]For details of the WannaCry ransomware attacks in 2017 and the cyberattack on Colonial Pipeline, see Paul Vigna, "Hackers Just Stole $66,000 in Bitcoin. Now What?" *Wall Street Journal*, May 16, 2017, https://www.wsj.com/articles/hackers-just-stole-66-000-in-bitcoin-now-what-1494937394; and Collin Eaton and Dustin Volz, "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom," *Wall Street Journal*, May 19, 2021, https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

Figure 3.2.1. Cyberattacks on Crypto Assets and Cyber Run Risk of Stablecoins

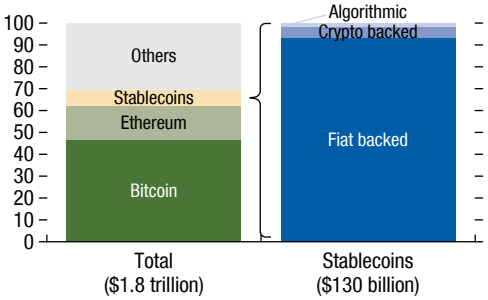
Crypto assets are vulnerable to cyberattacks and are frequently used to make ransomware payments.

1. Value Stolen in Crypto Hacks and Crypto Value Received by Ransomware Attackers



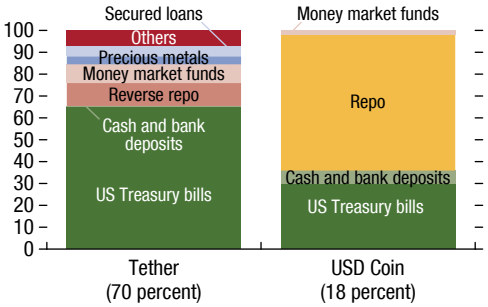
Stablecoins represent about 10 percent of the crypto market, and most of them are fiat-backed ...

2. Crypto Market Capitalization, December 2023
(Distribution, percent)



... which increases their link to the traditional financial system through asset holdings.

3. Reserves of Fiat-Backed Stablecoins, December 2023
(Distribution, percent)



Sources: Chainalysis; CoinGecko; DefiLlama; disclosure statements of stablecoins; and IMF staff calculations.
Note: In panel 2, the numbers in parentheses under the *x* axis labels indicate the total market capitalization of crypto assets and stablecoins as of December 31, 2023; In panel 3, the numbers in parentheses represent the share of Tether and USD Coin in all stablecoins as of December 31, 2023.

Box 3.2 *(continued)*

they are increasingly connected with the traditional financial sector. The current stablecoin market is dominated by fiat-backed stablecoins designed to mirror the values of traditional currencies like US dollars and euros (Figure 3.2.1, panel 2) by holding assets such as US Treasuries, money market funds, and bank deposits, often with high levels of concentration (Figure 3.2.1, panel 3). A major cyber incident affecting such a stablecoin could lead to it depegging from the underlying asset, creating run risk and forced sales of financial assets that could ultimately spill over to the financial system (Adachi and others 2020; Ma, Zeng, and Zhang 2023).[4] For example, in August 2022, hackers exploited a bug in a newly deployed liquidity pool, resulting in the minting of 3 billion Acala USD and the depegging of Acala USD from the US dollar, with substantial outflows from the crypto-backed stablecoin protocol (see Online Annex 3.8). The run, however, did not result in significant spillovers to the financial system.[5]

Institutional investors have been increasingly investing in crypto assets (Huang, Lin, and Wang 2022), and some large banks may also have nontrivial crypto exposures, both direct and through assets under custody (Bank for International Settlements 2023b).[6] Because the prices of crypto assets tend to drop significantly after a cyberattack (Milunovich and Lee 2022; Chen, Chang, and Yang 2023),[7] monitoring of crypto exposures is warranted to preserve financial stability.[8]

[4]The total amount of fiat-backed stablecoin reserves is comparable to the average daily transaction volume of US Treasury bills—about $120 billion in 2022, according to the Securities Industry and Financial Markets Association, https://www.sifma.org/resources/research/us-treasury-securities-statistics/.

[5]For details of this incident, see Gareth Jenkinson, "Another Depeg: Acala Trace Report Reveals 3B aUSD Erroneously Minted," *Cointelegraph*, August 17, 2022, https://cointelegraph.com/news/another-depeg-acala-trace-report-reveals-3b-ausd-erroneously-minted.

[6]On January 10, 2024, the Securities and Exchange Commission approved the listing and trading of a number of spot bitcoin exchange-traded products (https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023).

[7]Cyberattacks on crypto assets could affect the price of crypto assets by (1) placing a large amount of stolen cryptocurrency on the market that results in short-term oversupply, (2) disrupting market infrastructures, and (3) adversely affecting investor sentiment through the theft of personal financial information.

[8]In this context, in December 2022, the Basel Committee on Banking Supervision finalized standards for banks on how to monitor and manage exposures to crypto assets. These standards revised the Basel Committee's prudential regulations, specifying how banks should treat crypto asset exposures. Although the standards are effective immediately, they lack legal force, prompting the Basel Committee to urge national regulators to implement the standards by 2025. For details, see Bank for International Settlements (2022).

References

Adachi, Mitsutoshi, Matteo Cominetta, Christoph Kaufmann, and Anton van der Kraaij. 2020. "A Regulatory and Financial Stability Perspective on Global Stablecoins." Macroprudential Bulletin 10–1, European Central Bank, Frankfurt, Germany.

Adelmann, Frank, Jennifer A. Elliott, Ibrahim Ergen, Tamas Gaidosch, Nigel Jenkinson, Tanai Khiaonarong, Anastasiia Morozova, Nadine Schwarz, and Christopher Wilson. 2020. "Cyber Risk and Financial Stability: It's a Small World After All." IMF Staff Discussion Note 2020/007, International Monetary Fund, Washington, DC.

Adrian, Tobias, and Caio Ferreira. 2023. "Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards." *IMF Blog*, March 2. https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards

Afonso, Gara, Filippo Curti, and Atanas Mihov. 2019. "Coming to Terms with Operational Risk." Liberty Street Economics (blog), *Federal Reserve Bank of New York*, January 7. https://libertystreeteconomics.newyorkfed.org/2019/01/coming-to-terms-with-operational-risk.html

Aldasoro, Iñaki, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach. 2022. "The Drivers of Cyber Risk." *Journal of Financial Stability* 60 (C, June): 100989.

Amir, Eli, Shai Levi, and Tsafrir Livne. 2018. "Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets." *Review of Accounting Studies* 23 (3): 1177–1206.

Bank for International Settlements. 2022. "Prudential Treatment of Cryptoasset Exposures." Basel, Switzerland.

Bank for International Settlements. 2023a. "Central Bank Digital Currency (CBDC) Information Security and Operational Risks to Central Banks." Basel, Switzerland.

Bank for International Settlements. 2023b. "Basel III Monitoring Report." Basel, Switzerland.

Bank of Canada. 2023a. "Financial System Survey Highlights—2023." Ottawa, Canada. https://www.bankofcanada.ca/2023/05/financial-system-survey-highlights-2023/

Bank of Canada. 2023b. "Financial System Review—2023." Ottawa, Canada. https://www.bankofcanada.ca/2023/05/financial-system-review-2023/

Bank of England. 2023. "Systemic Risk Survey Results–2023 H2." London, United Kingdom. https://www.bankofengland.co.uk/systemic-risk-survey/2023/2023-h2

Bank of England. 2024a. "Financial Stability in Focus: The FPC's Macroprudential Approach to Operational Resilience." London, United Kingdom. https://www.bankofengland.co.uk/financial-stability-in-focus/2024/march-2024.

Bank of England. 2024b. "The Financial Policy Committee's Medium-Term Priorities (2023–2026)." London, United Kingdom. https://www.bankofengland.co.uk/about/people/financial-policy-committee/priorities.

Bank of France. 2022. "Assessment of Risks to the French Financial System." Paris, France. https://www.banque-france.fr/system/files/2023-04/2022_s2_ers_final-en.pdf

Bank of Mexico. 2022. "Financial Stability Report." Mexico City, Mexico.

Basel Committee on Banking Supervision. 2021. "Principles for Operational Resilience." Basel, Switzerland. https://www.bis.org/bcbs/publ/d516.pdf

Boukherouaa, El Bachir, and Ghiath Shabsigh. 2023. "Generative Artificial Intelligence in Finance: Risk Considerations." IMF Fintech Note 2023/006, International Monetary Fund, Washington, DC.

Boukherouaa, El Bachir, Ghiath Shabsigh, Khaled AlAjmi, Jose Deodoro, Aquiles Farias, Ebru S. Iskender, Alin T. Mirestean, and Rangachary Ravikumar. 2021. "Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance." IMF Departmental Paper 2021/024, International Monetary Fund, Washington, DC.

Bouveret, Antoine. 2018. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment." IMF Working Paper 2018/143, International Monetary Fund, Washington, DC.

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

Center for Strategic and International Studies. 2020. "The Hidden Costs of Cybercrime." Washington, DC.

Chen, Yu-Lun, Yung Ting Chang, and Jimmy Yang. 2023. "Cryptocurrency Hacking Incidents and the Price Dynamics of Bitcoin Spot and Futures." *Finance Research Letters* 55 (B): 103955.

Committee on Payments and Market Infrastructures and International Organization of Securities Commission (CPMI-IOSCO). 2016. "Guidance on Cyber Resilience for Financial Market Infrastructures." Bank for International Settlements, Basel, Switzerland. https://www.bis.org/cpmi/publ/d146.pdf

Committee on Payments and Market Infrastructures and International Organization of Securities Commission (CPMI-IOSCO). 2022. "Implementation Monitoring of the PFMI: Level 3 Assessment on Financial Market Infrastructures' Cyber Resilience." Bank for International Settlements, Basel, Switzerland.

Crosignani, Matteo, Marco Macchiavelli, and André Silva. 2023. "Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains." *Journal of Financial Economics* 147 (2): 432–48.

Depository Trust and Clearing Corporation (DTCC). 2023. "Systemic Risk Barometer: 2023 Risk Forecast." New York. https://www.dtcc.com/-/media/downloads/Systemic-Risk/Systemic-Risk-2023

Deep Instinct. 2023. "Generative AI and Cybersecurity: Bright Future or Business Battleground?" Voice of SecOps, 4th ed., New York.

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

Duffie, Darrell, and Joshua Younger. 2019. "Cyber Runs." Hutchins Center Working Paper 51, Brookings Institution, Washington, DC.

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee. 2022. "Cyber Risk and the US Financial System: A Pre-Mortem Analysis." *Journal of Financial Economics* 145 (3): 802–26.

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee. 2023. "When It Rains, It Pours: Cyber Risk and Financial Conditions." Staff Report 1022, Federal Reserve Bank of New York.

Ernst & Young/Institute for International Finance (EY/IIF). 2024. "Managing through Persistent Volatility: The Evolving Role of the CRO and the Need for Organizational Agility." 13th Annual EY/IIF Global Bank Risk Management Survey." Washington, DC.

European Central Bank (ECB). 2022. "Financial Stability Review, November 2022." Frankfurt, Germany. https://www.ecb.europa.eu/pub/financial-stability/fsr/html/ecb.fsr202211~6383d08c21.en.html

European Systemic Risk Board (ESRB). 2020. "Systemic Cyber Risk." Fitch Ratings. Exploring Bank Cybersecurity Risk. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

Financial Stability Board. 2023. "Final Report on Enhancing Third-Party Risk Management and Oversight–A Toolkit for Financial Institutions and Financial Authorities." Basel, Switzerland.

Financial Stability Oversight Council (FSOC). 2023. "Annual Report." US Department of the Treasury, Washington, DC. https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michale Weber. 2023. "Cybersecurity Risk." *Review of Financial Studies* 36 (1): 351–407.

Gaidosch, Tamas, Frank Adelmann, Anastasiia Morozova, and Christopher Wilson. 2019. "Cybersecurity Risk Supervision." IMF Departmental Paper 2019/014, International Monetary Fund, Washington, DC.

Group of Seven. 2016. "G7 Fundamental Elements of Cybersecurity for the Financial Sector." https://assets.publishing.service.gov.uk/media/5a7f840bed915d74e33f6e9f/G7_Fundamental_Elements_Oct_2016.pdf.

Group of Seven. 2017. "G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector." https://assets.publishing.service.gov.uk/media/63dcd7e58fa8f57fbfff3db9/2017-10-26-g7-fundamental-elements-cybersecurity-data.pdf

Group of Seven. 2018. "G-7 Fundamental Elements for Threat-LED Penetration Testing." https://assets.publishing.service.gov.uk/media/63dcd69fe90e075d9e6926ea/2018-10-24-g7-fundamental-elements-led-penetration-testing-data.pdf

Group of Seven. 2020. "G-7 Fundamental Elements of Cyber Exercise Programmess." https://assets.publishing.service.gov.uk/media/5fe4852c8fa8f56af53c5d77/G7_Fundamental_Elements_of_Cyber_Exercise_Programs_October_2020.pdf

Group of Seven. 2022a. "G7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector." https://assets.publishing.service.gov.uk/media/63dcd54bd3bf7f070ffc1e87/2022-10-13-g7-fundamental-elements-third-party-risk.pdf

Group of Seven. 2022b. "G7 Fundamental Elements of Ransomware Resilience For The Financial Sector." https://assets.publishing.service.gov.uk/media/63dcd4fde90e075d9ff98162/2022-10-13-g7-fundamental-elements-ransomware-data.pdf

Harry, Charles, and Nancy Gallagher. 2018. "Classifying Cyber Events." *Journal of Information Warfare* 17 (3): 17–31.

He, Zhiguo, Sheila Jiang, Douglas Xu, and Xiao Yin. 2023. Rev. ed. "Investing in Lending Technology: IT Spending in Banking." NBER Working Paper 30403, National Bureau of Economic Research, Cambridge, MA.

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Adriana Tache. 2018. "The Future of Financial Stability and Cyber Risk." Brookings Institution, Washington, DC.

Huang, Xiaoran, Juan Lin, and Peng Wang. 2022. "Are Institutional Investors Marching into the Crypto Market?" *Economics Letters* 220 (C): 110856.

International Association of Insurance Supervisors (IAIS). 2016. "Issues Paper on Cyber Risk to the Insurance Sector." Basel, Switzerland.

International Association of Insurance Supervisors (IAIS). 2023. "Issues Paper on Insurance Sector Operational Resilience." Basel, Switzerland.

International Organization of Securities Commissions (IOSCO). 2021. "Principles on Outsourcing Final Report." Madrid. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf

Jamilov, Rustam, Hélène Rey, and Ahmed Tahoun. 2023. "The Anatomy of Cyber Risk." NBER Working Paper 28906, National Bureau of Economic Research, Cambridge, MA.

Kamiya, Shinichi, Kang Jun-Koo, Kim Jungmin, Andreas Milidonis, and René M Stulz. 2021. "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms." *Journal of Financial Economics* 139 (3): 719–49.

Kashyap, Anil K., and Anne Wetherilt. 2019. "Some Principles for Regulating Cyber Risk." *AEA Papers and Proceedings* 109 (May): 482–87.

Kopp, Emanuel, Lincoln Kaffenberger, and Christopher Wilson. 2017. "Cyber Risk, Market Failures, and Financial Stability." IMF Working Paper 2017/185, International Monetary Fund, Washington, DC.

Ma, Yiming, Yao Zeng, and Anthony Zhang. 2023. "Stablecoin Runs and the Centralization of Arbitrage." Unpublished.

Microsoft. 2023. "Microsoft Digital Defense Report." Redmond, WA. https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MDDR_FINAL_2023_1004.pdf

Milunovich, George, and Seung Ah Lee. 2022. "Measuring the Impact of Digital Exchange Cyberattacks on Bitcoin Returns." *Economics Letters* 221 (C): 110893.

Modi, Kosha, Nicola Pierri, Yannick Timmer, and Maria Soledad Martinez Peria. 2022. "The Anatomy of Banks' IT Investments: Drivers and Implications." IMF Working Paper 2022/244, International Monetary Fund, Washington, DC.

Moody's. 2023. "Cyber Budgets Increase, Executive Overview Improves, but Challenges Lurk under the Surface." Special Report, New York. https://www.moodys.com/web/en/us/about/insights/data-stories/2023-cyber-survey-highlights.html

Office of the President of the United States. 2022. "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems." National Security Memo, White House Briefing Room, Washington, DC. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

Sedik, Tahsin, Majid Malaika, Michel Gorbanyov, and Jose Deodoro. 2021. "Quantum Computing's Possibilities and Perils." *IMF Blog*, September.

Statista. 2022. "Cybercrime Expected to Skyrocket in Coming Years." https://cdn.statcdn.com/Infographic/images/normal/28878.jpeg

SWIFT. 2023. "Swift Customer Security Controls Framework v2024." La Hulpe, Belgium. https://www2.swift.com/knowledgecentre/rest/v1/publications/cscf_dd/48.0/CSCF_v2024_20230707.pdf?logDownload=true

US Department of the Treasury. 2022. "Annual Report." Washington, DC.

US Department of the Treasury. 2023. "The Financial Services Sector's Adoption of Cloud Services." Washington, DC. https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

US Government of Accountability Office (US GAO). 2021. "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response." *WatchBlog*, April 22. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

World Economic Forum (WEF). 2023. "The Global Risks Report 2023." 18th ed. Cologny, Switzerland.