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

¹The 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.

²The 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.
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

3Direct 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.
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

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

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...
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/IIIF 2024). Mentions of cyber risks have surged in firms’ earnings 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/cd287352-23eb-48d8-a82b-6eb713b80962).
Central banks and financial regulators are viewing cybersecurity as a material risk. 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). 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).  

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 release, increasing market volatility (Kristztian 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).  

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 resiliency 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.  

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 supervisors increasingly consider cyber risk in financial stability reports and supervisory stress tests (Figure 3.3, panel 3, green bars). 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).  

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 release, increasing market volatility (Kristztian 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).  

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 resiliency 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.  

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. 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 Wetherit 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.

Transmission of Cyber Risks to Macrofinancial Stability

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

1. Financial market events: Cyber incidents can lead to financial market disruptions, such as stock market crashes, derivatives price spikes, and other market interventions.
2. Economic instability: Cyber incidents can spread throughout the economy, leading to supply chain disruptions, reduced consumer spending, and other economic downturns.
3. Financial stress: Cyber incidents can cause financial institutions to fail, leading to systemic risk and potential for a financial crisis.

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 firms and financial stability, focusing on sectors such as financial services, retail, and healthcare. For example, Duffie and Younger (2019) show the possibility of cyberattacks leading to a systemic shock. Focusing on the financial sector, 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, Kover, 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 firms 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.
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

Sources: Adelmann and others 2020; and IMF staff.
Note: AI = artificial intelligence; FMIs = financial market infrastructures; IT = information technology.
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). Most notably, through generative AI (GenAI), more sophisticated phishing messages or deepfakes could be used for identity theft or fraud (Boukherouaa and Shabsigh 2023). 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. 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. 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.

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. 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

---

11AI 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.

12In 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).


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

15For 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.

16The 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.
cyber incidents because equity markets are forward looking and reflect market participants’ assessment of firms’ value (Kamiya and others 2021). The analysis reveals that when controlling for market movements and other relevant factors, stock prices do not on average react strongly to cyber incidents ...

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.
Chapter 3: Cyber Risk: A Growing Concern for Macroeconomic Stability

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.

1. Abnormal Returns, All Cyber Incidents

2. Abnormal Returns, Malicious Cyber Incidents

3. Abnormal Returns, Malicious Cyber Incidents, Small 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). 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.

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.

Econometric analysis suggests that digitalization and geopolitical tensions significantly raise the...
After the pandemic, however, the probability of such incidents possibly because they relied more on IT infrastructure. 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. 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). By contrast, firms in countries with more developed cyber legislation are less likely to be targets of a cyber incident.

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 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 incidents declined. 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 their 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.

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

---

22To 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.

23The 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.

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

25Geopolitical 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.

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

27Cyber 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.

28The 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).

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

   Banks (total)  | Banks (G-SIBs)  | Insurers  | Asset managers  | Other financial  | IT  | Other non-financial

   - Higher cyber vulnerability

   - Median and interquartile range

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

   - Asset size
   - Country-level concentration
   - Global concentration
   - Payment activity
   - Asset under custody

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

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 expense has 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).
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). In addition, Figure 3.9, panel 2, shows that smaller banks are more susceptible to outflows after cyber incidents, suggesting that such

35In 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.\textsuperscript{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).\textsuperscript{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).\textsuperscript{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).\textsuperscript{39}

The rapid evolution of fintech introduces additional cyber risks.\textsuperscript{40} Fintech firms have increased the financial system’s exposure to cyber threats through their digitalized operations and interconnectedness.\textsuperscript{41} Decentralized finance—crypto-market-based financial intermediation—has grown rapidly since 2020 and cyberattacks on decentralized finance, which employs

\textsuperscript{36} “Wholesale deposits” are defined as deposits from private nondepository institutions.

\textsuperscript{37} More specifically, the “reverse outflow rate” represents outflows from deposits with a maturity of less than 30 days (or undetermined maturity).

\textsuperscript{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.

\textsuperscript{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).

\textsuperscript{40} Fintech (financial technology) is technological innovation in financial activities (see Chapter 3 of the April 2022 Global Financial Stability Report).

\textsuperscript{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.

\textsuperscript{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.

\textsuperscript{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)
   - AEs
   - EMDEs

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

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

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

   - No/ongoing discussion
   - Within the next 12 months
   - Yes

   - 2021
   - 2023

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

4. Frequency Distribution of Cyber Preparedness Index Score
   (Percent)
   - Below 1
   - 1–2
   - 2–3
   - 3–4
   - 4–5
   - Higher index range

   - 2021
   - 2023

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

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

   - All respondents
   - Latin America
   - Europe
   - Asia
   - Africa

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

   (Percent)

   - Africa
   - Asia
   - Europe
   - Latin America

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.\(^4^4\)
- 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.\(^4^5\)
- Formal cyber risk stress tests remain less common, with 27 percent of the surveyed economies including cyber risk in their stress test programs.\(^4^6\) 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.\(^4^7\) 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.\(^4^8\) Lack of awareness, resources constraint, and competing priorities often hinder further progress.

\(^4^4\)Regular cyber tests include vulnerability assessments, penetration testing, and red team testing (that is, threat intelligence-based testing).

\(^4^5\)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.

\(^4^6\)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.

\(^4^7\)See Online Annex 3.7 for a detailed explanation of the construction of the Cybersecurity Preparedness Index.

\(^4^8\)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 Miţov 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.

49According 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.
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...
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

¹The 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).


³A 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, and on major crypto assets (such as bitcoin and ether). For example, in 2014, the crypto exchange Mt. Gox suffered a loss of $850,000,000 in 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. 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.

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.


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). 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

4The 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/.


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


7Cyberattacks 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.

8In 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


