SECTION 5
Operational Risk

- **Operational risk remains one of the most critical risks to banks.**
- **Geopolitical events continue to increase the likelihood of cyber attacks on banks.**
- **The banking industry's software infrastructure remains vulnerable to cyber attacks, including ransomware attacks and threats against third-party service providers.**
- **Robust customer due diligence (CDD) policies and anti-money laundering (AML) and countering the financing of terrorism (CFT) compliance programs reduce the U.S. financial system's susceptibility to illicit financial activity risks.**

Operational risk remains one of the most critical risks to banks. The increase in the number and sophistication of cyber attacks poses serious challenges to operational risk management across the banking industry. According to a bank risk management survey, cybersecurity risk was the top near-term risk for banks.[110] Technology advances require bank managers to continuously improve cybersecurity and other internal controls to create operational resilience and mitigate the risk that their bank will suffer a significant service disruption.

In 2022, geopolitical events continued to increase the likelihood of cyber attacks on banks. The Microsoft Digital Defense Report, published in November 2022, stated that cyber attacks targeting critical infrastructure for many firms around the world jumped from 20 percent of all nation-state attacks to 40 percent. This large increase in malicious activity was attributed to Russia's attempts to damage Ukrainian infrastructure, along with aggressive espionage targeting of Ukraine's allies, including the United States.[111]

The banking industry's information technology infrastructure remains vulnerable to cyber attacks, including ransomware attacks and threats against third-party providers. Ransomware continues to pose a significant threat to U.S. critical infrastructure sectors, including finance and banking, as the number of attacks continue to increase. Ransomware is a form of malicious software designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Reports of such attacks as of 2021 exceeded recent year totals (Chart 44). Ransomware has the potential to disrupt core business activities, resulting in operational outages. It can also result in an inability to access critical business and customer data. Banks reduce the risk of a ransomware attack's success and minimize its negative impacts by applying effective cybersecurity risk management and mitigation principles.

Ransomware typically leverages known software vulnerabilities, compromised credentials, or phishing emails targeting bank employees to gain access to networks through remote access channels. Ransomware developers and operators continue to advance their tactics and tools and offer their services to others using a Ransomware-as-a-Service model.

Cyber threats to third-party providers of software, hardware, and computing services remain an important source of risk to the financial industry (inset box). Security risks arising from compromised third-party software include disclosure of credentials or confidential data, corruption of data, installation of malware, and application outages. These problems can result in lost time, money, and customer trust. In addition, supply chain attacks on third-party software and computing services have the potential to

[110] Andrés Portilla, Martin Boer, and Hillary Veals, "12th Annual EY-IIF Bank Risk Management Survey," January 11, 2023.

[111] Microsoft, "Microsoft Digital Defense Report 2022," November 7, 2022.

negatively affect the security and operations of a bank. IBM's annual Cost of a Data Breach Report showed one in five data breaches were due to a software supply chain compromise.[112] The threat of compromise from Log4J (a ubiquitous Java-based script) vulnerabilities that can allow access to network operations and data lingers. As of November 2022, security firms estimate approximately one-third of all downloads of the script were still pulling a vulnerable version. The U.S. government has warned that the "endemic" script is expected to persist "in the wild" for at least a decade.[113]

Quantum computing will pose new risks to critical infrastructure systems.

While quantum computing promises greater computing speed and power, it also has the potential to render current encryption methods vulnerable. In general, traditional encryption relies on complex mathematical problems (encryption algorithms) that take an immense amount of time for classic computers to solve without knowing the encryption key. However, quantum computers use a different computing architecture that can solve certain types of problems much faster, including some encryption algorithms. With the release of quantum computing to the public, current encryption methods may become inadequate.[114]

Money laundering is also a key component of operational risk. Money laundering, which is the practice of filtering illicit proceeds through a series of transactions in order to camouflage the illegal nature of the funds, continues to pose risks to the banking industry because it facilitates and conceals crime. Further, the United States is vulnerable to terrorist financing and other forms of illicit finance because much of the global economy is interconnected with the U.S. economy and financial system. The federal banking agencies, in conjunction with the U.S Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), are updating their AML/CFT program regulations to address priorities identified by FinCEN.[115] FinCEN recognizes that not every priority will be relevant to every bank, but each bank should review and incorporate, as appropriate, each priority based on the bank's broader risk-based AML/CFT program. Banks need not incorporate the priorities into their risk-based AML/CFT programs until the effective date of the final revised regulations.

If a bank does not know the customer with whom a bank is conducting business, the U.S. financial system is more susceptible to money laundering, terrorist financing, and other illicit financial activity risks. Banks implement CDD policies, procedures, and processes to assess and mitigate risks associated with customers and the products and services offered by the bank. Still, the inability to know the beneficial owner of accounts maintained at U.S. financial institutions presents risk to the U.S. financial system. In 2016, the United States implemented the beneficial ownership rule requiring financial institutions to identify and verify beneficial owners of legal entity customers when a new account is opened. This approach will change once the Corporate Transparency Act (CTA) is fully implemented. The CTA will require certain companies to disclose to FinCEN their beneficial ownership information when they are formed (or for non-U.S. companies, when they register with a state to do business in the United States); they will also be required to report changes in beneficial owners. Beneficial ownership information helps address the risk within the United States, whereby criminals have historically been able to take advantage of the lack of uniform laws and regulations pertaining to the disclosure of an entity's beneficial owners.[116] These revisions are expected to help facilitate law enforcement investigations and make it more difficult

[112] IBM, "Cost of a Data Breach Report 2022," July 2022.

[113] Cyber Safety Review Board, "Review of the December 2021 Log4j Event," July 11, 2022.

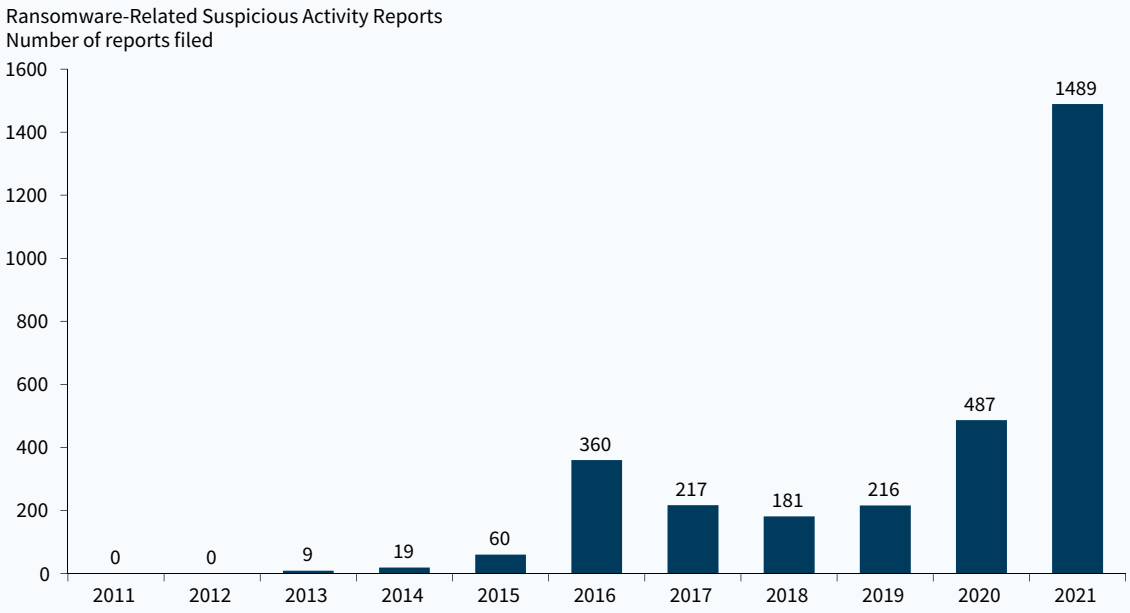
[114] Cybersecurity and Infrastructure Security Agency, "Preparing Critical Infrastructure for Post-Quantum Cryptography," CISA Insights, August 2022.

[115] Financial Crimes Enforcement Network, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," U.S. Department of the Treasury, June 30, 2021.

[116] U.S. Department of the Treasury, "2022 National Money Laundering Risk Assessment," February 2022.

CHART 44

Ransomware Attacks Increased Significantly in Recent Years



Source: Financial Crimes Enforcement Network.
Note: Annual data from 2011 to December 2021.

for illicit actors to hide behind corporate entities registered in the United States or foreign entities registered to do business in the United States.[117]

Bank reliance on third parties to perform AML/CFT compliance services or act as an intermediary between the bank and its customers may be a source of risk. Third parties used by a bank may not be subject to AML/CFT laws and regulations. Excessive use of third-party relationships can limit bank staff's knowledge of customer account activity and impede the ability to verify the identity of a customer or beneficial owner of a legal entity customer, perform CDD procedures, or identify the beneficiary or recipient of a financial transaction, product, or service.

The dynamic nature of sanctions regulations increases the risk that banks process transactions for a sanctioned party. Financial authorities and governments use economic and trade sanctions based on foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime. Since Russia's invasion of Ukraine, the Office of Foreign Assets Control (OFAC) and the Department of State issued approximately 1,500 new and 750 amended sanctions (i.e., changes to sanctions programs). Inadequate interdiction software implementation, ineffective supplemental processes (manual or automated), unknown gaps in sanctions screening systems, and untimely updates to a bank's interdiction software increase the risk of processing transactions for a sanctioned party.[118] The FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) issued joint alerts urging banks to be vigilant against efforts by individuals or entities to evade BIS export controls implemented in connection with the Russian Federation's invasion of Ukraine.[119]

[117] Ibid.

[118] Interdiction software screens and detects transactions associated with parties recorded on the Specially Designated Nationals and Blocked Persons List issued by the OFAC and sanctions lists from other relevant jurisdictions.

[119] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," FIN-2022-Alert003, June 28, 2022; and "Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts," FIN-2023-Alert004, May 19, 2023.