REPORT TO CONGRESS

Cybersecurity and Financial System Resilience Report

July 2024

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

The Federal Reserve System is the central bank of the United States. It performs five key functions to promote the effective operation of the U.S. economy and, more generally, the public interest.

The Federal Reserve

- **conducts the nation's monetary policy** to promote maximum employment and stable prices in the U.S. economy;
- **promotes the stability of the financial system** and seeks to minimize and contain systemic risks through active monitoring and engagement in the U.S. and abroad;
- **promotes the safety and soundness of individual financial institutions** and monitors their impact on the financial system as a whole;
- **fosters payment and settlement system safety and efficiency** through services to the banking industry and U.S. government that facilitate U.S.-dollar transactions and payments; and
- **promotes consumer protection and community development** through consumer-focused supervision and examination, research and analysis of emerging consumer issues and trends, community economic development activities, and administration of consumer laws and regulations.

To learn more about us, visit www.federalreserve.gov/aboutthefed.htm.

Contents

Overview

The Consolidated Appropriations Act, 2021[1] (CAA) requires the Board of Governors of the Federal Reserve System (Board) to submit annually for seven years a report focused on cybersecurity to Congress. The CAA calls for a description of measures the Board has undertaken to strengthen cybersecurity within the financial services sector and with respect to the Board's functions as a regulator, including the supervision and regulation of financial institutions and third-party service providers. Pursuant to the CAA, this report is organized in three main sections covering:

- the Board's policies and procedures related to cybersecurity risk management, including with respect to the Board's supervision and regulation of financial institutions, the Board's administration of its internal information security program, and the Reserve Banks' information security program;
- Board activities to address cybersecurity risks, including those carried out through our supervision of financial institutions, through the Board's own programs and initiatives, and through those of the Reserve Banks as a provider of critical payment and settlement services; and
- current and emerging cyber threats that may pose a risk to the resilience of the financial system.

As described in the report, the Board views cybersecurity as a high priority for the Federal Reserve System (System) and Board-supervised institutions. The Board and the Reserve Banks maintain robust information security programs and engage and coordinate on cybersecurity issues with numerous critical stakeholders including the financial regulatory agencies and industry. These efforts include actively monitoring cybersecurity threats and responding, as appropriate, to incidents that could affect the operations of the Board, the Reserve Banks, or Board-supervised institutions.

[1] Consolidated Appropriations Act, Pub. L. No. 116-260, Division Q, section 108 (2021).

Board Policies and Procedures for Cybersecurity Risk Management

The Board recognizes the increasing and evolving nature of cybersecurity threats to the financial system. Accordingly, the Board's supervision and regulation of financial institutions encompasses review and monitoring of institutions' cybersecurity risk management and information technology (IT) programs. As part of its safety and soundness supervision, the Board issues cybersecurity-related regulations and guidance, examines and monitors supervised institutions' cybersecurity risk-management posture, and collects data on cyber incidents (along with the other federal financial regulatory agencies) to monitor trends in the financial services sector. Additionally, the Board and the Reserve Banks secure their internal information and information systems through robust cybersecurity risk-management programs. The Board follows the Federal Information Security Modernization Act (FISMA) requirements, and the Reserve Banks also employ a framework based on the National Institute of Standards and Technology's (NIST) standards and guidance.

Board Supervisory Policies and Procedures

The Board's supervisory policies and examination procedures are aimed at reducing the risk of cybersecurity threats to the financial system through effective cybersecurity practices at supervised institutions. The Board issues and publishes rules and guidance for supervised institutions regarding IT risk management, cybersecurity, operational resilience, third-party risk management, and other related topics.[2]

The Board has established enforceable guidelines that require banks to have internal controls and information systems appropriate to the size of the institution and to the nature, scope, and risk of its activities and that provide for, among other requirements, effective risk assessment and adequate procedures to safeguard and manage assets. The guidelines also require banks to have internal audit systems that provide for adequate testing and review of information systems.[3] Additionally, the Interagency Guidelines Establishing Information Security Standards require banking organizations to develop and implement administrative, technical, and physical safeguards to promote the security, confidentiality, and integrity of customer information.[4]

---

[2] See Board of Governors of the Federal Reserve System, "Information Technology Guidance," last modified February 4, 2022, https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm and Board of Governors of the Federal Reserve System, "Operational Resilience," last modified February 4, 2022, https://www.federalreserve.gov/supervisionreg/topics/operational-resilience.htm.

[3] See 12 C.F.R. pt. 208, appendix D-1, Interagency Guidelines Establishing Standards for Safety and Soundness.

[4] See 12 C.F.R. pt. 208, appendix D-2; 12 C.F.R. pt. 225, appendix F. These requirements of banking organizations are promulgated pursuant to title V, subtitle A, of the Gramm-Leach-Bliley Act.

The Board also issues guidance on these topics. For example, the "Interagency Paper on Sound Practices to Strengthen Operational Resilience" contains information for large banks on how to manage cyber risk and assess cybersecurity preparedness for their critical activities.[5] See table 1 for recent Board actions and actions in collaboration with other financial regulatory agencies to promote cybersecurity.

Table 1. Recent Board and interagency actions to promote cybersecurity since August 2023

Date	Action
March 8, 2024	The Board issued updates to the operational risk-management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board, known as Regulation HH (Financial Market Utilities). FMUs provide essential infrastructure to clear and settle payments and other financial transactions upon which the financial markets and the broader economy rely to function effectively. The amendments provide additional clarity and specificity to existing requirements in four key areas of operational risk management: incident management and notification; business continuity management and planning; third-party risk management; and review and testing of operational risk-management measures.[1]
May 7, 2024	The Board, together with the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC), issued an interagency third-party risk management guide for community banks (guide) to assist community banks when developing and implementing their third-party risk-management practices. The guide, which supplements the Interagency Guidance on Third-Party Relationships: Risk Management, • offers potential risk-management considerations, including those related to cybersecurity and operational risks throughout the stages of the third-party relationship life cycle, which include planning, due diligence, contract negotiation, ongoing monitoring, and termination; • includes potential sources of information to inform risk-management decisions, including those related to technology risk management; and • describes different risk-management scenarios through illustrative examples.

[1] See Financial Market Utilities, 89 Fed. Reg. 18749 (Mar. 15, 2024), https://www.federalregister.gov/documents/2024/03/15/2024-05322/financial-market-utilities.

Board Internal Policies and Procedures

The Board continues to take a proactive approach to safeguarding its operations and assets by developing, documenting, and implementing a comprehensive security program. The program is designed to protect both the information and information systems that support the agency's core mission functions. The Board's information security program follows federal information security requirements as established by FISMA and related NIST standards.

In accordance with the President's "Executive Order on Improving the Nation's Cybersecurity,"[6] the Board is taking steps to further improve its security posture by implementing the latest

[5] See Board of Governors of the Federal Reserve System, "SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience", published on November 2, 2020. https://www.federalreserve.gov/supervisionreg/srletters/SR2024a1.pdf.

[6] See The White House, "Executive Order on Improving the Nation's Cybersecurity," last modified on May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

cybersecurity standards and principles. One key area of focus is the adoption of zero-trust principles,[7] which has further enhanced the Board's cybersecurity posture by requiring users to continuously verify credentials when using internal resources. A second area of focus is supply chain risk management (SCRM), which will ensure Board information and services remain secure even as we leverage third parties to store and process our information.

The Board's Office of Inspector General (OIG) performs independent and regular assessments of the agency's security programs, practices, and systems. Furthermore, the Board also collaborates with cybersecurity consultants and experts, who provide independent recommendations on improving the Board's cybersecurity controls and protocols.

In addition to administering the agency's information security program, the Board also oversees the cyber-risk management posture of the Reserve Banks. The Reserve Banks have a comprehensive, risk-based information security program that is informed by NIST standards and guidance and industry best practices. The Reserve Banks, as operators of critical financial services, proactively provide tools and communications aimed at mitigating cyber risks to their financial institution customers. Additionally, Federal Reserve Operating Circular No. 5, Electronic Access, sets forth the information security requirements applicable to institutions accessing Reserve Bank services, such as the Fedwire Funds Service, Fedwire Securities Service, FedACH, FedNow Service, and National Settlement Service.[8] Under Operating Circular No. 5, institutions are required to implement technical, operational, managerial, and procedural controls designed to protect the security of the IT environment, including systems and processes that are used to access Reserve Bank services and applications.

[7] See OMB, M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[8] See "Federal Reserve Banks Operating Circular No. 5 Electronic Access," effective May 1, 2024, https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/050124-operating-circular-5.pdf.

Board Activities to Address Cybersecurity Risks

The Board's activities help confirm that policies, procedures, rules, and guidance for supervised institutions and internal agency functions are successfully implemented. The Board's approach includes providing appropriate cybersecurity-related staffing, training, and resources for bank examiners. The OIG also conducts independent reviews of the Board focused on continually improving cybersecurity supervisory activities and enhancing the Board's internal processes. The Board's activities involve interagency, intergovernmental, industry, and international collaboration.

Supervisory Activities

The Federal Reserve conducts examinations and monitoring of cybersecurity risk management, governance, and controls at supervised institutions. It also examines and monitors, pursuant to the Board's authority under the Bank Service Company Act (BSCA),[9] certain services performed on behalf of financial institutions by their service providers. The Federal Reserve's supervision activities in this area promote financial institutions' ability to protect against cyber incidents and other hazards, safeguard critical infrastructure, and address emerging technology risks. Federal Reserve examination staff use the Uniform Rating System for Information Technology (URSIT) and the FFIEC IT Handbook, which is informed by NIST standards and guidance along with other sources, in conducting cybersecurity and other information technology-related examinations.[10]

Examiners evaluate cybersecurity with consideration of the business models and activities conducted by supervised institutions as part of a principles-based supervision program. The scope of any specific examination considers key cybersecurity risks, the industry landscape, and other factors such as emerging technologies. As part of these evaluations, examiners consider business-line controls, risk-management practices, assurance functions, and governance activities performed by the firm's senior management and board of directors.

For the eight U.S. global systemically important banks, the Federal Reserve conducts joint cybersecurity examinations or coordinated cyber reviews with the OCC and FDIC. Additionally, for large

[9] 12 U.S.C. §§ 1861-67.

[10] See Federal Financial Institutions Examination Council, "FFIEC Information Technology Examination Handbook Infobase," https://ithandbook.ffiec.gov/.

financial institutions with assets of $100 billion or more,[11] the Federal Reserve conducts "horizontal" cybersecurity examinations across several institutions at once. Horizontal examinations promote consistency in the assessment of cyber governance and controls across firms, identify the range of practices observed at firms, and, as appropriate, allow the Federal Reserve to issue supervisory findings when weaknesses are present. In addition to the horizontal reviews, supervisory teams monitor cyber, IT, and operational risk using continuous monitoring processes as well as monthly engagement focused on emerging threats.

For community banking organizations (those with under $10 billion in assets) and regional banking organizations (those with $10 to $100 billion in assets), URSIT is the primary mechanism to inform evaluations of cybersecurity practices and assign IT ratings to each firm. If deficiencies in an institution's cybersecurity program are identified, examiners may issue supervisory findings that could impact the URSIT rating or result in enforcement action. Firms are expected to promptly address findings to ensure appropriate protection against cyber threats.

For community banking organizations and regional banking organizations, the Board follows a risk-focused approach that assigns examination resources to higher-risk banks and areas of each bank's operations and encourages banks to maintain risk-management capabilities appropriate to their size and complexity. Cybersecurity practices are evaluated with standardized procedures through regular IT examinations. For state member banks, these examinations are often conducted jointly with state banking regulators. The Federal Reserve along with the FDIC and state banking authorities use the Information Technology Risk Examination Program (InTREx), which provides supervisory staff with risk-focused and efficient examination procedures for assessing IT and cybersecurity risks at supervised institutions. InTREx procedures may also be used in conjunction with those listed in the FFIEC IT Handbook[12] when a financial institution's risk or complexity is elevated.

The Federal Reserve expects financial institutions to effectively manage risks associated with their third-party service providers. Additionally, the BSCA provides authority for the federal banking agencies (FBAs)[13] to regulate and examine certain services performed by third parties on behalf of insured depository institutions and their affiliates. The FBAs jointly supervise a subset of third-party technology service providers through an interagency technology service provider supervision program, which incorporates a risk-based process for selecting service providers for inclusion in the program. Through examinations of service providers in the program, the agencies issue an

[11] A LISCC firm is a firm that is supervised under the Large Institution Supervision Coordinating Committee supervisory program. Current LISCC firms are Bank of America Corporation; The Bank of New York Mellon Corporation; Citigroup, Inc.; The Goldman Sachs Group, Inc.; JPMorgan Chase & Co.; Morgan Stanley; State Street Corporation; and Wells Fargo & Company. An LFBO firm refers to a domestic or foreign banking organization with combined U.S. assets of $100 billion or more that is supervised under the Large and Foreign Banking Organization supervisory program.

[12] See Federal Financial Institutions Examination Council, "FFIEC Information Technology Examination."

[13] The federal banking agencies are the Board, OCC, and FDIC.

URSIT rating evaluating each service provider. As part of the examination program, the agencies conduct cybersecurity-specific examinations of these service providers which informs their overall URSIT rating. The agencies issue reports of examination, communicate supervisory findings, and take enforcement actions when needed. The report of examination is distributed on a confidential basis to the service provider and to the provider's client financial institutions to assist with their ongoing monitoring of third-party risk.

In addition, the Federal Reserve's consumer compliance supervision program complements the IT and cybersecurity reviews conducted by safety and soundness examiners to ensure that supervised institutions maintain systems and processes to protect customers' sensitive personal financial information. Through this program, the Federal Reserve's examiners evaluate the effectiveness of supervised institutions' compliance with consumer financial privacy laws and regulations.[14]

With regard to financial market utilities (FMUs), the Board has direct supervisory authority for a subset of the FMUs designated by the Financial Stability Oversight Council (FSOC). The Board also works closely with staff at the Federal Reserve Banks of New York and Chicago, as well as at the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC), to oversee the other designated FMUs which are not directly supervised by the Board. Specific focus is placed on FMUs' operational and cyber-risk management programs.[15] The Board regularly sets supervisory priorities for and examines (or participates in CFTC- and SEC-led examinations of) designated FMUs' operational risk-management frameworks.[16] The Board also reviews proposed changes to designated FMUs' rules, procedures, and operations, including proposed changes that would materially affect a designated FMU's operational and cyber-risk management. An example of this is Regulation HH (Financial Market Utilities), mentioned in the previous section.[17]

The Federal Reserve uses the ORSOM (Organization; Risk Management; Settlement; Operational Risk and Information Technology (IT); and Market Support, Access, and Transparency) rating system in its assessment of designated FMUs for which the Board is the supervisory agency under title VIII of the Dodd-Frank Act. The rating system facilitates discussion of the FMU's condition with the FMU's management and board of directors. Supervisory staff explain to the FMU the

[14] Examples include Regulation P (12 C.F.R. pt. 1016.) and the "red flags" rule under the Fair Credit Reporting Act (15 U.S.C. § 1681m(e)).

[15] See Board of Governors of the Federal Reserve System, "Designated Financial Market Utilities," last modified January 29, 2015, https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm.

[16] Under section 807(d) of the Dodd-Frank Act, the Board may, at its discretion, participate in any title VIII examination led by the SEC or CFTC. 12 U.S.C § 5466)(d)(2).

[17] See Financial Market Utilities, 79 Fed. Reg. 3666 (April 15, 2024), https://www.federalregister.gov/documents/2024/03/15/2024-05322/financial-market-utilities.

factors that determine that FMU's rating, including operational risks and IT, which covers cyber risk.[18]

Furthermore, as part of the Board's supervisory activities, the Federal Reserve has established processes and programs to monitor and share information involving cybersecurity threats, vulnerabilities, and incidents. Additionally, the Federal Reserve monitors cybersecurity developments and events across the financial services sector, including payment, clearing, and settlement systems. The Federal Reserve proactively educates examination staff on cyber threats or vulnerabilities. This helps examination staff to evaluate risks to supervised institutions and inform supervisory engagement. The Board also receives notifications from banking organizations about cyber incidents that may affect the U.S. banking system as part of the Computer-Security Incident Notification Rule.[19] This rule requires a banking organization to notify its primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after the banking organization determines that a cyber incident has occurred. The federal bank regulatory agencies have been receiving notifications from banking organizations since the promulgation of this rule in 2021.

Incident Response Efforts

The Federal Reserve's supervisory incident response processes enable an effective and repeatable supervisory response to cyber incidents that affect Federal Reserve-supervised institutions and service providers. The Board and other FBAs require a banking organization to notify its primary regulator of computer-security incidents that rise to the level of a notification incident within 36 hours of determining that such an incident has occurred. A bank service provider is required to notify affected banking organization customers as soon as possible regarding certain computer-security incidents so the customer banking organizations can determine whether a notification incident has occurred.[20] The notifications help the agencies become aware of and react to emerging threats.[21] Under Regulation HH, a designated FMU for which the Board is the supervisory agency is required to immediately notify the Board of material operational incidents. Additionally, Regulation HH requires a designated FMU to establish criteria and processes for providing timely communication and responsible disclosure, such that it provides (1) immediate notice to affected participants in the event of actual disruptions or material degradation to its critical operations or services or to its ability to fulfill its obligations on time and (2) timely notice to participants and other relevant entities of all other material operational incidents that require immediate notifica-

---

[18] For designated FMUs that are primarily supervised by the CFTC or SEC, Federal Reserve supervisory staff communicate assessments of the FMU's cyber-risk management to the CFTC or SEC, as appropriate.

[19] See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66,424 (April 1, 2022), https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.

[20] See 12 C.F.R. pt. 53.

[21] See Board of Governors of the Federal Reserve System, "Contact Information in Relation to Computer-Security Incident Notification Requirements," SR letter 22-4 (March 29, 2022), https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm.

tion to the Board, taking into account the risks and benefits of disclosure to the designated FMU and to participants and other relevant entities.[22]

Cybersecurity-Related Findings

As part of the Board's safety and soundness supervision, Federal Reserve supervisors examine and monitor the information security practices and cybersecurity programs of supervised institutions and may issue supervisory findings notifying supervised institutions of identified deficiencies. The Federal Reserve requires supervised institutions to respond appropriately to cybersecurity-related supervisory findings and take proactive steps to mitigate cyber risk. When institutions do not address findings in an appropriate period of time, the Board has tools such as informal and formal enforcement actions to ensure institutions operate in a safe and sound manner.

Staffing, Training, and Deployment of Examiner Resources

The Federal Reserve maintains an experienced, trained complement of supervision staff with IT expertise, including individuals with expertise in cybersecurity. Federal Reserve examiners assess supervised institutions' cyber and information security practices, internal audit, risk management, and controls to ensure that institutions implement appropriate and effective safeguards to mitigate cyber risk. For large domestic firms and service providers, using a risk-based approach, examiners are assigned to a specific firm or group of firms, and for foreign entities and smaller domestic institutions, examiners are assigned on a portfolio basis.

The Federal Reserve has established frameworks to guide the recruitment and assignment of examiners, including IT and cybersecurity risk specialists. The Federal Reserve coordinates and conducts training and makes available to staff a learning platform with an extensive catalogue of cyber, IT, and information security training. We also leverage conferences and training hosted by the FFIEC and government agencies. In addition, Federal Reserve examiners participate in other conferences and training events to gain perspective from external cybersecurity practitioners and industry experts. Internal groups at the Federal Reserve serve as useful forums to share information and institutional knowledge of cyber resilience issues, including committees that address operational resilience matters across the portfolios supervised by the Federal Reserve. The Federal Reserve continues to assess and offer cyber skills training aligned with risks to supervised institutions.

[22] See 12 C.F.R. pt. 234.

Board OIG Efforts Related to Supervisory Activities

On June 26, 2023, the OIG issued the report, *Results of Scoping the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions*.[23] The report identified findings and recommendations to improve the effectiveness of the cybersecurity incident response process including updating guidance to clarify the mission and governance structure and enhancing guidance and training. The Board has addressed the six areas needing improvement and is working with the OIG to close the recommendations from this report.

In 2020, the OIG issued a report identifying opportunities for the Board to enhance cybersecurity supervision of LISCC firms related to governance, ratings, and training.[24] The Board successfully addressed the areas needing improvement. As of September 2022, all recommendations from this report were closed by the OIG.

In 2017, the OIG conducted an evaluation to assess the Board's cybersecurity examination approach and to determine whether the Board was providing effective oversight of supervised institutions' information security controls and cybersecurity risk for select oversight areas.[25] The Board successfully addressed all areas and all recommendations except for one, where the OIG had recommended that the Board reiterate to financial institutions the requirement under the BSCA to notify their primary regulator of the existence of new service relationships. The Board continues to coordinate with the other FBAs to clarify, reiterate, and improve compliance with this requirement.

Reserve Bank Activities

In addition to administering the Board's internal cybersecurity program, the Board also supervises the Reserve Banks' IT operations and oversees the implementation and management of cybersecurity across the Federal Reserve System. With cyber-attacks increasing in scale and severity, the Reserve Banks recognize that a major incident within their enterprise can have a severe impact on the economy and the stability of the financial sector. While the threat level to the Reserve Banks remains elevated, the System continues to maintain robust protective operations, invest in risk-mitigation initiatives and programs, and continuously monitor and assess cybersecurity risks to critical systems and sensitive data. For example, the Reserve Banks continue to strengthen their security posture by implementing several high-priority cybersecurity initiatives that include enhancing identity and access management capabilities, improving the ability to respond to

---

[23] See Board of Governors of the Federal Reserve System, Office of Inspector General, *Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions* (Washington: Board of Governors, June 2023), https://oig.federalreserve.gov/reports/board-cyber-incident-response-jun2023.htm.

[24] See Board of Governors of the Federal Reserve System, Office of Inspector General, *The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced* (Washington: Board of Governors, September 2020), https://oig.federalreserve.gov/reports/board-cybersecurity-supervision-LISCC-firms-sept2020.htm.

[25] See Board of Governors of the Federal Reserve System, Office of Inspector General, *The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing* (Washington: Board of Governors, April 2017), https://oig.federalreserve.gov/reports/board-cybersecurity-supervision-apr2017.htm.

evolving cybersecurity threats and system vulnerabilities, monitoring and mitigating risks posed by vendors and service providers, and focusing on controls that align with the pillars of a zero-trust architecture. Additionally, with increasing ransomware activity in the financial sector, the Reserve Banks continue to take actions to strengthen their processes, infrastructure, and controls to further enhance ransomware protections and response capabilities consistent with federal and industry guidance on mitigating these risks.

The Reserve Banks have also focused their efforts on bolstering the security of the U.S. payment system. This includes enhancing the resiliency and cybersecurity posture of Federal Reserve Financial Services through efforts to improve resiliency and recovery capabilities. These improvements include enhancing procedures in place to ensure the resiliency of payment platforms that are routinely tested across a variety of contingency situations to help ensure resumption of critical operations in the event of a local, regional, or widespread disruption. The suite of applications that make up the payment system and associated recovery processes are regularly evaluated and enhanced to address emerging risk scenarios, such as those that might occur during a cyber event.

Finally, the Reserve Banks stay abreast of enacted federal laws on cybersecurity and executive orders focused on cybersecurity and resiliency through monitoring by the Board. Examples include the Cybersecurity and Infrastructure Security Agency's (CISA) proposed incident reporting rule under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA Act) and the 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[26] Through these efforts, the Reserve Banks work together and with government partners to further enhance the state of information security and resiliency across the System.

Coordination Activities

Due to the high degree of interconnectedness of the global financial system, the Board is an active participant and leader in domestic and international forums addressing the cyber resiliency of the financial services sector. Board and Federal Reserve System staff work together to coordinate with other domestic and international agencies, governance bodies, financial regulators, and industry to share information and best practices as well as publish guidance for regulated entities.

Intergovernmental Coordination

To strengthen risk-management practices across the financial services sector and reduce the effects of cyber-related incidents, the Board coordinates with partners through the President's Working Group on Financial Markets (PWGFM), the Financial and Banking Information Infrastructure Committee (FBIIC), and the Federal Financial Institutions Examination Council (FFIEC).

[26] See The White House "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," October 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

The Board is a member of the PWGFM, whose mission is to enhance the integrity, efficiency, orderliness, and competitiveness of the nation's financial markets and their ability to maintain investor confidence. A significant part of this mission is related to cyber and other operational risks.

The Board is also a member of the FBIIC, which is chartered under the PWGFM. The FBIIC consists of federal and state financial regulatory agencies that supervise banking, investment, and insurance firms, and is chaired by the U.S. Department of the Treasury (Treasury). FBIIC members engage in efforts to strengthen the security and resiliency of critical infrastructure across the financial services sector including financial institutions regulated and supervised by the FBIIC member organizations. In the past several years, the FBIIC has engaged in a number of areas relating to cybersecurity, cloud adoption, data protection, and incident response. For example, the Federal Reserve participated in cloud security initiatives as a follow-up to the Treasury's report exploring how the use of cloud services may affect the sector's operational resilience and incident response.[27]

The Board participates in the FBIIC's periodic cyber exercises that include participation from regulatory agencies, financial institutions, and trade associations. These exercises have proved useful in advancing incident management and information-sharing protocols across the financial services sector. Additionally, through participation in these exercises, the Board has improved its ability to respond to, in coordination with other financial regulators, potential operational disruptions in the financial services sector's critical infrastructure. These exercises also have led to the creation of private sector-led and public sector-supported initiatives to enhance cyber resiliency. These include continued adoption of a capability to enable participating financial institutions to store critical customer account data in a secure industry-standard format, and capabilities to proactively identify, analyze, and coordinate activities to mitigate systemic risk to the U.S. financial system (and other critical infrastructure) from cyber threats.

In addition, as a member of the FFIEC, which is an interagency body that promotes uniformity and consistency in the examination of financial institutions across its members, the Board actively coordinates with other FFIEC members on cybersecurity risk-management issues. The Board contributes to the efforts of the FFIEC in responding to cyber incidents affecting institutions supervised by FFIEC members. The Board also contributes to the FFIEC's efforts and supports ongoing dialogue on cybersecurity issues and opportunities to improve consistency in examination approaches. The Board has contributed to work on a number of FFIEC subcommittees:

- The Cybersecurity and Critical Infrastructure Subcommittee (CCIS) continued to work on key cybersecurity areas, including risk management and oversight, threat intelligence and collaboration, cybersecurity controls, and cyber-incident management and resilience. The CCIS continues

[27] See U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services* (Washington: Department of the Treasury, February 2023), https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

to focus its efforts on U.S. government cybersecurity harmonization efforts, ransomware threats, and SCRM.

- The CCIS continued to issue messages on significant cybersecurity issues and information to supervised institutions. The messages addressed issues related to cyber- and supply chain attacks involving extortion to raise awareness of evolving threat risks as well as associated considerations of enhanced fraud controls, regulatory reporting, customer notification, and other compliance issues.
- In August 2023, the FFIEC IT Subcommittee sponsored its annual IT Conference for examiners that highlighted current and emerging technology issues affecting supervised institutions, including cybersecurity attack techniques and impacts from geopolitical events, learning from ransomware incidents, security for "the internet of things," SCRM and software bill of materials, IT asset management, operational resilience, and third-party risk management. The conference was attended by more than 500 examiners from federal and state regulatory agencies.
- In recognition of National Cybersecurity Awareness Month, the CCIS hosted an Industry Outreach webinar focusing on ransomware in November 2023. During the event, CCIS representatives highlighted ransomware trends, supervisory observations, and related FFIEC guidance.
- In 2024, the Board participated in the FFIEC's temporary subcommittee related to community bank and credit union digitalization. The aim of the subcommittee is to research and identify challenges, which may result in safety and soundness concerns, that community banks and credit unions experience when adopting technology solutions involving digitalization. The subcommittee's work plans include, but will not be limited to, issues relating to core service providers and relationships with other third-party technology vendors.

Additionally, the Board coordinated through the Cybersecurity Forum for Independent and Executive Branch Regulators to increase the overall consistency and effectiveness of cybersecurity regulation by federal regulatory authorities. The Board worked with the Department of Homeland Security as they developed their report to Congress, *Harmonization of Cyber Incident Reporting to the Federal Government*, which is required by the CIRCIA Act.[28] Additionally, the Board coordinated and consulted with CISA on the draft notice of proposed rulemaking,[29] as required by the CIRCIA Act, for cyber-incident reporting.

The Board continued to engage with efforts such as the NIST Cybersecurity Framework (CSF). The CSF 2.0 update was completed and issued in February 2024.[30] Board and Federal Reserve

---

[28] See U.S. Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government* (Washington: Department of Homeland Security, September 2023), https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.

[29] See Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (proposed April 4, 2024), https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

[30] See "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, February 26, 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

System staff participated in NIST outreach sessions for the issuance of CSF 2.0. The CSF 2.0 update aims to keep pace with the evolving cybersecurity landscape and helps banking organizations strengthen cyber-risk management and reduce those risks with customized measures. Banks that adopt a standardized approach to cybersecurity preparedness are better able to track their progress over time and share information and best practices with other financial institutions and regulators.

The Board also continued to follow CISA's development of cross-sector cyber performance goals (CPGs), voluntary practices that businesses and critical infrastructure owners can take to protect themselves against cyber threats. As recommended by Board staff and others, CISA reorganized and reissued the CPGs in March 2023 to align to the NIST CSF. Additionally, the Board is monitoring the release by CISA of financial sector-specific CPGs that are planned for release in 2024.

Public and Private Sector Coordination

The Board participates in various public-private partnerships to enhance cyber resilience in the financial system. Through FBIIC, the Board coordinates with the Financial Services Sector Coordinating Council (FSSCC), a nonprofit body composed of more than 70 members from across the financial services industry whose mission is to strengthen the resiliency of the financial services sector. This partnership focuses on improving the financial services sector's ability to rapidly respond to and recover from significant cybersecurity incidents, thereby reducing the potential for such incidents to threaten the stability of the financial system and the broader economy. In 2023, joint FBIIC and FSSCC priorities included hardening the sector's defenses against increasing cyber threats, including those arising from the Russian invasion of Ukraine; assessing cloud security risks; and exercising cyber-incident response plans.

The Board participated in the Cloud Executive Steering Group, a public-private partnership of FBIIC and FSSCC members formed by the Treasury at the direction of the FSOC to address gaps identified in the February 2023 Treasury report entitled *The Financial Services Sector's Adoption of Cloud Services*.[31] This report—developed in coordination with members of the FBIIC and FSSCC—assesses the current state of cloud adoption in the financial services sector and the potential benefits and challenges of increased adoption of cloud-based technologies by the sector.

The Board participated in industry-led initiatives to enhance cybersecurity risk management. For example, the Board is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), the global financial industry's resource for cyber- and physical–threat intelligence analysis and sharing. The Board encourages its supervised institutions to incorporate threat monitoring programs and participate in information sharing organizations such as the FS-ISAC. Outside of FS-ISAC, the Board also participates in other information sharing and analysis organizations

[31] See U.S. Department of the Treasury, *The Financial Services Sector's*.

(ISAOs), which include trade associations, third-party threat intelligence services, and specialized information sharing arrangements. The Board encourages voluntary cybersecurity information sharing through CISA's Joint Cyber Defense Collaborative and CISA Central, which are both platforms for sharing situational awareness and response efforts to current cyber, communications, and physical incidents.

The Board also participated in the planning and execution of public-private "Hamilton Series" cyber exercises lead by the Treasury with other U.S. government agencies, the FSSCC, and FS-ISAC to develop cyber exercises aimed at improving responses to a range of cyber-threat scenarios within the U.S. financial sector. In 2024, the Board, along with the Treasury, facilitated in-person tabletop exercises with participants from smaller banking organizations as part of the Hamilton Series. These cyber exercises better prepare the financial and public sectors to respond to cyber-attacks.

International Coordination

The Board leads or contributes to cybersecurity activities undertaken by groups such as the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), the Committee on Payment and Market Infrastructures (CPMI) (and its joint efforts with the International Organization of Securities Commissions (IOSCO)), the International Association of Insurance Supervisors (IAIS), and the Group of Seven (G7).

In light of the threats cyber incidents pose to the interconnected global financial system, the FSB has assumed a key role in promoting cyber resilience. The Board contributed to the FSB's work to promote greater convergence in cyber-incident reporting by

- setting out recommendations to address the issues identified as impediments to achieving greater harmonization in cyber-incident reporting;[32]
- enhancing the FSB's Cyber Lexicon to include additional terms related to cyber-incident reporting; and [33]
- developing a concept for a common format for incident reporting exchange (FIRE) to establish a standard, voluntary framework for financial institutions' incident information.[34]

In addition, the FSB continues its work to enable the financial system to adapt to structural changes in relation to strengthening financial institutions' ability to manage third-party and out-

[32] See Financial Stability Board, *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report*, (Basel: Financial Stability Board, April 2023), https://www.fsb.org/wp-content/uploads/P130423-1.pdf.

[33] See "Cyber Lexicon," Financial Stability Board, last modified April 2023, https://www.fsb.org/wp-content/uploads/P130423-3.pdf.

[34] See "Format for Incident Reporting Exchange (FIRE): A possible way forward," Financial Stability Board, last modified on April 13, 2023, https://www.fsb.org/wp-content/uploads/P130423-2.pdf.

sourcing risk.[35] On December 4, 2023, the FSB published its toolkit for enhancing third-party risk management and oversight, which was developed in response to concerns over the risks to financial institutions from outsourcing and third-party service relationships.[36] The toolkit aims to strengthen financial institutions' ability to manage third-party risks and financial authorities' ability to monitor and strengthen the resilience of the financial system and to reduce fragmentation in regulatory and supervisory approaches.

The BCBS acts as the primary forum for international coordination on the prudential regulation of banks and cooperation on banking supervisory matters. In March 2021, the BCBS issued the Principles for Operational Resilience[37] and the Principles for the Sound Management of Operational Risk.[38] These documents highlight the importance of sound operational risk management, including cyber-risk management, and are aligned with guidance released by the Board on operational resilience.[39] In September 2021, the BCBS published a newsletter calling for increased efforts to improve banks' resilience to cyber threats, intended to complement earlier actions and promote widespread adoption of measures to strengthen banks' cybersecurity.[40] Currently, the BCBS is considering an update to the 2005 Joint Forum Paper on Outsourcing, which is related to third-party risk.[41]

Through the CPMI-IOSCO, the Board has played a key role in the development of the Principles for Financial Market Infrastructures (PFMI) and related guidance for FMIs, including the Cyber Resilience Guidance. The CPMI-IOSCO continues to monitor and analyze emerging risks that could affect the safety and efficiency of FMIs, including cyber risk and third-party risk. The Board contributes to the development of IAIS's annual key financial stability priorities for insurance providers, which was most recently released in January 2024. Among the priorities is a focus on growing cyber risks, which continues to create significant impacts to insurers' financial liabilities. In 2023, the Board contributed to the International Association of Insurance Supervisors' *Global Insurance*

---

[35] See Financial Stability Board, "Enhancing Third-Party Risk Management and Oversight," Discussion Paper (Basel: Financial Stability Board, June 2023), https://www.fsb.org/wp-content/uploads/P220623.pdf.

[36] See Financial Stability Board, "Enhancing Third-Party Risk Management and Oversight", December 4, 2023, https://www.fsb.org/wp-content/uploads/P041223-1.pdf.

[37] See Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Basel: Bank for International Settlements, March 2021), https://www.bis.org/bcbs/publ/d516.pdf.

[38] See Basel Committee on Banking Supervision, *Revisions to the Principles for the Sound Management of Operational Risk* (Basel: Bank for International Settlements, March 2021), https://www.bis.org/bcbs/publ/d515.pdf.

[39] See Board of Governors of the Federal Reserve System, "Interagency Paper on Sound Practices to Strengthen Operational Resilience," SR letter 20-24 (November 2, 2020), https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm.

[40] See Bank for International Settlements, "Basel Committee Calls for Improved Cyber Resilience, Reviews Climate-Related Financial Risks and Discusses Impact of Digitalization," news release, September 20, 2021, https://www.bis.org/press/p210920a.htm.

[41] See the Basel Committee on Banking Supervision, *Outsourcing in Financial Services* (Basel: Bank for International Settlements, February 2005), https://www.bis.org/publ/joint12.pdf. See the Basel Committee on Banking Supervision, "Basel Committee approves disclosure framework and capital standard for banks' cryptoasset exposures and amendments to interest rate risk in the banking book standard, and agrees to consult on third-party risk principles," news release, July 3, 2024, https://www.bis.org/press/p240703.htm.

Market Report.[42] This analysis focuses on risks and trends associated with cyber insurance coverage, cyber resilience in the insurance sector, and the impact these risks may have on financial stability.

Given the rapidly evolving nature of cyber risks and the cross-border and cross-sector relevance of cyber threats, the Board continued to participate in the G7 Cyber Expert Group, a working group established by the G7 finance ministers, central bank governors, and other financial authorities to elevate cybersecurity concerns and enhance cooperation among G7 jurisdictions and the financial services sector. The working group has published papers on cybersecurity topics, including a paper calling for common categorizations of malicious cyber incidents and other operational IT incidents to aid in comparing and studying incidents across jurisdictions.[43]

The Board contributed to current G7 cyber priorities, including coordinating responses to ransomware incidents, cyber-incident response across jurisdictions, and cyber risks from third-party service providers and emerging technologies. In 2024, the Board also participated in the planning and execution of a cross-border coordination exercise to bolster the financial sector's resilience across all G7 jurisdictions in response to a widespread cyber incident affecting the financial system. The exercise assumed a large-scale cyber-attack on financial market infrastructures and entities in all G7 jurisdictions and brought together 23 financial authorities, including ministries of finance, central banks, bank supervisors, and market authorities, as well as private industry participants.

Board Internal

The Board places a strong emphasis on promoting cyber-risk management through active collaboration and coordination across agency stakeholders. To achieve this goal, the Board's Office of the Chief Operating Officer (OCOO) facilitates timely exchange of information regarding cyber-risk issues across divisions, including business, IT, and information security functions. This approach ensures that cross-functional perspectives are taken into account, enabling the Board to coordinate its efforts and develop cohesive cybersecurity policy. Board security personnel take an active role in other coordination activities, collaborating with groups within the System, as well as participating in interagency cybersecurity forums and working groups facilitated by CISA. This collaboration helps Board staff better identify and respond to potential threats. The Board is an active participant in CISA's Continuous Diagnostics and Mitigation (CDM) program, which is a government-wide effort to improve cybersecurity risk management across all federal agencies. The CDM

[42] See International Association of Insurance Supervisors, *Global Insurance Market Report (GIMAR), Special Topic Edition on Cyber*, (Basel: International Association of Insurance Supervisors, April 2023) https://www.iaisweb.org/uploads/2023/04/GIMAR-2023-special-topic-edition-on-cyber.pdf.

[43] See Cyber Expert Group, "Proposal for a Common Categorization of IT Incidents," April 6, 2021, https://acpr.banque-france.fr/sites/default/files/medias/documents/20210406_occasional_paper_categorisation_incidents.pdf.

provides tools and services to help agencies identify and prioritize cybersecurity risks, improve visibility into their networks, and make informed decisions about how to address those risks.

Board OIG Assessment of the Board's Progress in Implementing Key FISMA Information Security Program Requirements

To support the annual independent evaluation of agency information security programs by inspectors general (IGs) under the Federal Information Security Modernization Act (FISMA), the Department of Homeland Security publishes FISMA reporting metrics. These metrics direct IGs to evaluate the effectiveness of agency information security programs across various attributes grouped into eight security domains.[44] These domains align with the five security functions defined by the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): *identify, protect, detect, respond, and recover*.[45] Pursuant to the FISMA reporting metrics, IGs assess the effectiveness of each of the five NIST Cybersecurity Framework function areas using a maturity model spectrum. The five levels of the IG FISMA maturity model are: ad hoc (level 1), defined (level 2), consistently implemented (level 3), managed and measurable (level 4), and optimized (level 5). Within the context of the maturity model, a level 4 information security program is considered to be operating at an effective level of security. While more work needs to be done, the Board OIG's 2023 assessment of the Board's overall information security program rated the program as continuing to operate effectively at a level 4 maturity.[46] The Board will continue to prioritize the protection of its operations and assets through ongoing assessments and improvements of its security posture.

The Board's Ongoing Efforts to Strengthen Its Information Security Program

The Board also places a strong emphasis on maintaining a comprehensive security and privacy control program, which is supported by a centralized Plan of Action and Milestones (POA&M) process. This process ensures that plans are developed in response to any finding or weakness identified in security and privacy control implementations. In addition, the POA&M process is used to track and report on the remediation of findings and status of recommendations issued by the OIG, as well as weaknesses identified through internal controls testing. Board staff plan to continue to work on making progress on closing outstanding POA&Ms.

---

[44] See "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0," Cybersecurity and Infrastructure Security Agency, last modified on April 17, 2020, https://www.cisa.gov/sites/default/files/publications/FY_2020_IG_FISMA_Metrics.pdf.

[45] See "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

[46] See Board of Governors of the Federal Reserve System, Office of Inspector General, *2022 Audit of the Board's Information Security Program* (Washington: Board of Governors, September 2022), https://oig.federalreserve.gov/reports/board-information-security-program-sep2022.pdf.

The Board continues to take steps to improve its cybersecurity posture and protect against cyber threats. These steps include investing in technical controls such as firewalls, intrusion detection and prevention systems, and security information and event management systems to monitor and detect potential threats. The Board follows FISMA and related NIST standards and guidance and implements the necessary controls to protect our information systems. In addition, the Board engages with third-party security experts to perform regular assessments and penetration testing to identify opportunities to improve its security posture. Finally, the Board has implemented a layered security architecture, which includes multiple layers of defense such as network segmentation, access controls, and encryption to better protect non-public information.

The Board also continues to work on many efforts to enhance its information security architecture. Indeed, one of the Board's top priorities includes the continued implementation of a zero-trust security model, which will provide an additional layer of security to protect its systems and data, as well as implementing web application security measures to identify and address vulnerabilities in the Board's web applications. The Board is also continuing work to enhance its existing supply chain risk-management policies and procedures to account for necessary security requirements for cloud systems and capabilities, such as updates to the Board's incident response and data protection policies.

Current or Emerging Threats to Financial System Resilience

The Board actively monitors cyber risks and emerging threats through internal Federal Reserve programs and resources, the supervisory process, and coordination with financial regulatory agencies and other government agencies, as well as the private sector. Given the highly interconnected nature of the financial services sector and its dependencies on critical service providers, all participants in the financial system face cyber threats.

The rising number of advanced persistent threats increases the potential for malicious cyber activity within the financial sector. Combined with the increased internet-based interconnectedness between financial institutions and the increasing dependence on third-party service providers, these threats may result in incidents that affect one or more participants in the financial services sector simultaneously and have potentially systemic consequences. Such incidents could affect the ability of targeted firms to provide services and conduct business as usual, presenting a unique challenge to operational resilience. These incidents can also threaten the confidentiality, integrity, and availability of the targeted firm's data.

Given the evolving threat landscape and potential for exploitation of vulnerabilities, domestic financial institutions have maintained a heightened state of preparedness. The Board and other federal banking agencies are closely monitoring developments related to these threats and have not observed any material impacts to the financial sector.

Geopolitical Tensions

The financial sector is potentially vulnerable to foreign conflicts and the activities of nation-state actors, both directly and indirectly, because of the interconnectedness of global financial markets and reliance on international digital networks.[47] Adverse geopolitical events, such as the ongoing conflicts in Ukraine and Israel, increase the likelihood of cyber-attacks with the intent of disrupting critical infrastructure, including financial services, or undermining trust in public and private sector institutions. In particular, DDoS[48] attacks have been widely observed due to the relatively low sophistication the attacks require and their potential to disrupt the availability of information

[47] See U.S. Department of the Treasury, *2022 Annual Report: Financial Stability Oversight Council* (Washington: Department of the Treasury, 2022), https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf.

[48] NIST defines DDoS as a denial-of-service technique that uses numerous hosts to perform cyber-attacks. See "2023 Key Cybersecurity Takeaways" State of New Jersey, December 2, 2023, https://www.cyber.nj.gov/Home/Components/News/News/998/214 and U.S. Department of Homeland Security, *Homeland Threat Assessment 2024* (Washington: Department of Homeland Security, 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf.

systems if organizations do not have effective information security and resilience controls. Additionally, destructive malware tools and methods used to destroy or corrupt critical data have been employed and observed.[49] These methods are evolving in sophistication and capability. Many of the geopolitical tensions create motivations and opportunities for malicious actors aiming to employ cyber-attacks to advance or harm the interest of participants in these conflicts, such as by targeting financial infrastructure.

Cyber-Criminal Activity

The global cyber-criminal ecosystem continues to remain a top threat across geographies and industry sectors, including the financial sector within the United States. As ransomware and cyber extortion attacks persist, these attacks may disproportionately affect small community and regional banking organizations that may not have sufficient information security resources and capabilities to protect their banking systems against sophisticated actors.

Cyber-criminal methods and resource offerings that pose a risk to financial institutions' ability to operate and protect customer data may include:

- **Ransomware as a service (RaaS)**. The RaaS ecosystem, where threat actors create "franchised" variants of ransomware, remains dynamic with groups disbanding and sometimes rebranding under different names. Despite activity from law enforcement aimed at disrupting ransomware operations, attacks associated with RaaS increased year-over-year from 2022 to 2023 across sectors and geographies.[50] One potential reason for this increase is leaks of popular ransomware "builders" that have led to multiple groups using similar variants to conduct attacks.[51] In addition, attackers continue to evolve technical capabilities to increase the scope and scale of attacks. These technical capabilities include directing attacks towards virtualization[52] technology and leveraging zero-day vulnerabilities as observed in the campaign targeting Progress Software's MOVEit Transfer application.[53]
- **Phishing**. Threat actors continue to evolve their techniques for targeting email to establish initial access for future malicious activity and exfiltrate sensitive information. Attackers can target email for purposes of delivering malware, gaining access to organizational credentials through

[49] See Cybersecurity and Infrastructure Security Agency, "U.S. and International Partners Release Report on Russian Cyber Actors Using 'Infamous Chisel' Malware," news release, August 31, 2023, https://www.cisa.gov/news-events/news/us-and-international-partners-release-report-russian-cyber-actors-using-infamous-chisel-malware.

[50] See U.S. Department of Justice, "U.S. Department of Justice Disrupts Hive Ransomware Variant," news release, January 26, 2023, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

[51] See Cybersecurity and Infrastructure Security Agency, "Understanding Ransomware Threat Actors: LockBit," news release, June 14, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.

[52] See Cybersecurity and Infrastructure Security Agency, "ESXiArgs Ransomware Recovery Guidance," news release, February 7, 2023, https://www.cisa.gov/news-events/alerts/2023/02/07/cisa-and-fbi-release-esxiargs-ransomware-recovery-guidance.

[53] See Cybersecurity and Infrastructure Security Agency, "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability, news release, June 7, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

phishing, or other social engineering activities. Downstream impact could result in theft of organizational funds through attacks such as business email compromise (BEC) or deployment of ransomware. Examples of improved techniques include more efficient means of subverting security controls on endpoints, embedding quick-response (QR) codes within malicious messages, and intercepting one-time passwords from users.

- **Increasing commoditization of tools associated with cyber-crime.** In addition to RaaS, financially motivated threat actors are creating various "services" that are used within attacks against organizations that are part of or support the financial sector. Examples of these "services" include malware-as-a-service (MaaS) and phishing-as-a-service (PhaaS). Threat actors can leverage these "services" for a nominal amount of money, effectively enabling lower-tier attackers to conduct moderately sophisticated campaigns. Threat actors are also continuing to work together to increase the effectiveness of attacks. Examples of this cooperation include selling information among themselves or selling initial access into victim organizations.

Malicious actors may impact financial sector organizations through exploiting both "zero-day" (patches not available) and "n-day" (patches available but not yet applied) vulnerabilities.[54] The sharing of technical information by both threat actors and security researchers continues to shorten the window between patch availability and observed exploitation activity. As evidenced by the increasing number of published vulnerabilities year-over-year, organizations should regularly review and update IT systems and controls for security against evolving threats. This exploitation activity also emphasizes the importance of a defense-in-depth security posture where a breakdown in one control does not lead to widespread compromise.

DDoS attacks continued to evolve with threat actors leveraging different techniques. These techniques include identifying weaknesses in specific applications and protocol designs and then exploiting those flaws to impact the availability of information systems. Threat actors can also leverage an increasing number of DDoS services that are available for sale on dark web forums and marketplaces. Despite the evolution in techniques, the major anti-DDoS services currently remain relatively well-positioned to defend against these attacks.

Cyber Risks Associated with Third-Party Providers

Financial institutions are increasingly relying on third-party service providers for significant business functions. While there are benefits to the use of third-party services, there are also challenges in ensuring adequate oversight of critical services not performed directly within a financial institution. A cyber-attack against a software vendor providing proprietary or publicly available

[54] See Cybersecurity and Infrastructure Security Agency, "#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability," news release, November 21, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a.

software, or against another third party, can have a significant impact on client firms. In the past year, this interdependency risk has been highlighted by the attacks against trading platforms and multiple providers within the mortgage-servicing ecosystem.[55]

The ability of threat actors to breach software providers and subsequently compromise the providers' clients highlights the risks stemming from interdependency often associated with third-party vendor management and automated software updates. This includes software-as-a-service, an ongoing connection between a software provider and a client firm, where the product is updated remotely on a periodic basis. As the use of third-party software, particularly software-as-a-service, becomes increasingly common in banking, cybersecurity risks are multiplied.

Financial institutions' increasing dependency on third parties is also illustrated by such institutions moving critical services to remote cloud-computing platforms to gain benefits such as increased computing capacity, lower costs, and concentrated technical expertise. In 2023, the Treasury published a report outlining trends related to the adoption of cloud services by the financial services sector as well as potential risks and other challenges.[56] Various publications from other government sources, including the National Security Agency[57] and CISA,[58] highlight cloud attacks by malicious actors along with important cloud security practices. These practices include upholding the cloud share responsibility model, using secure cloud identity and access management practices, implementing network segmentation and encryption in cloud environments, and mitigating risks from managed service providers in cloud environments, among others.

Threat actors will likely increase focus on the integration points between on-premises technology and cloud technology. This focus could include attacks against federated identity providers, with the goal of gaining access to firm environments. Attackers could also exploit potential weaknesses in controls within cloud services that serve to separate individual client environments. These "tenant isolation controls" are intended to keep one cloud customer from accessing other cloud customers' data. An issue with these controls could allow threat actors to compromise the data of cloud customers.

The Federal Reserve continues to engage with the Treasury and other public and private sector partners to address risks associated with third-party dependencies.

---

[55] See Harry Robertson, "ION brings clients back online after ransomware attack – source," *Reuters*, February 7, 2023, https://www.reuters.com/technology/ion-starts-bring-clients-back-online-after-ransomware-attack-source-2023-02-07/. EquiLend hack raised costs as traders flew blind, sources say. See "Recent Cyberattacks Impact Financial Services Sector," State of New Jersey, February 22, 2024, https://www.cyber.nj.gov/Home/Components/News/News/1192/214.

[56] See U.S. Department of the Treasury, *The Financial Services Sector's*.

[57] National Security Agency, "NSA Releases Top Ten Cloud Security Mitigation Strategies," news release, March 7, 2024, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies/.

[58] Cybersecurity and Infrastructure Security Agency, "CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices," news release, March, 7, 2024, https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices.

Other Emerging Technology-Related Threats

Third-party service providers, including fintech firms, can offer consumers the potential for access to new or better services, but such arrangements also provide potential opportunity for malicious actors to gain access to private data. Specifically, such emerging technologies are often vulnerable to exploitation by tech-savvy hackers looking to profit from technical and financial vulnerabilities in these technologies. Of particular potential risk is the rapid adoption by financial institutions of application programming interfaces, which provide accessible gateways into firms' information (often relied on by fintech platforms for information sharing) and may increase the risk of data breaches, especially of customers' personal or sensitive information, if not effectively secured and permissioned.

Among emerging technology, artificial intelligence (AI), machine learning, and large language models present both promising opportunities and significant threats within the financial sector. The capacity for these models to analyze vast datasets and detect intricate patterns can positively influence understanding of markets and financial stability. These capabilities also introduce significant risks such as cybersecurity concerns, algorithmic bias, and questions of ethical use. As these systems continue to mature, it will be important to take steps to mitigate these risks.

Although the potential benefits of AI capabilities include intrusion detection and data loss protection, the adoption of AI tools by malicious actors presents emerging threats to financial sector organizations:

- Attackers can use generative AI to increase the effectiveness of social engineering campaigns, including phishing and text-based smishing attacks. This could enable threat actors to capture sensitive information including user credentials that can be used to conduct further steps in an attack chain.
- Voice-cloning services[59] can potentially enable threat actors to circumvent existing controls such as voice verification that some financial sector organizations use to protect customer accounts.
- While many large language models provide guardrails against using them for malicious purposes, threat actors could potentially circumvent the guardrails and use generative AI to write malware for use in their operations.

Quantum computing is another significant emerging risk area, as quantum computing capabilities could render current encryption standards used by financial institutions obsolete. The introduction of post-quantum cryptography will provide new solutions for protecting the integrity and confidentiality of data at rest and in transit but will also give threat actors new capabilities to avoid detection as well

[59] Michael Atleson, "Chatbots, deepfakes, and voice clones: AI deception for sale," *Business Blog*, March 20, 2023, https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale.

as permit data exfiltration. Several agencies have highlighted steps that institutions can take now to prepare for the cryptographic risks associated with quantum computing. For example, in 2023, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) published "Quantum-Readiness: Migration to Post-Quantum Cryptography," which informs institutions about quantum capabilities and promotes a proactive approach for institutions to take now by instituting a "Quantum-Readiness Roadmap" to prepare for post-quantum cryptography migration.[60]

Threats such as these highlight the importance of collective actions across the government and strong collaboration with the private sector in advancing measures to understand and mitigate risks. Cyber-risk mitigation and cyber resilience initiatives continue to be high priorities for the Federal Reserve. Through policymaking, supervision of financial institutions and other entities overseen or operated by the Federal Reserve, and internal policies aimed at mitigating cyber threats, the Federal Reserve continues to maintain a strong internal resilience posture and promote resilience across the financial sector as a whole.

[60] See National Security Agency, "Quantum-Readiness: Migration to Post-Quantum Cryptography," news release, August 21, 2023, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/.

Find other Federal Reserve Board publications at www.federalreserve.gov/publications/default.htm, or visit our website to learn more about the Board and how to connect with us on social media.

www.federalreserve.gov
0724