Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Cross-Cutting Issues in Cybersecurity: Financial Institutions

March 1, 2021

Financial institutions remain a prime target for many types of malicious actors in cyberspace. The types of data these institutions hold make them a target, in addition to their role in managing money. As a result, government and industry have security requirements for these institutions. Because many financial institutions make significant investments in cybersecurity, the financial sector as a whole may provide insights into novel attacks and potentially cost-effective mitigation strategies.

This Insight outlines the cybersecurity risk to the financial services industry and efforts by government and industry to address those risks.

Financial Institutions' Realms of Cybersecurity Risk

Financial institutions face three broad types of cybersecurity risk: operational, reputational, and systemic.

Definitions

Cybersecurity	Financial Institutions
A process involving the prevention of damage to, protection of, and restoration of computers, computer networks, information and communications technology, virtual systems, cyber-physical systems, digital services and software (including the information and data contained in those systems), and users.	Financial institutions comprise the financial series sector. These institutions include depository institutions (e.g., banks and credit unions), broker-dealers, investment funds and companies, insurance companies, payment processors, and other credit and financing organizations.

Source: CRS Analysis.

Operational Risk

Like any organization, financial institutions face operational risk from cyber threats. They engage in activities to protect their business information technology (IT) networks and their operational networks. Business networks (e.g., email systems and web portals), can be the initial point of entry for malicious

Congressional Research Service
https://crsreports.congress.gov
IN11621

actors. Other attacks may target operational networks of the financial institution. Once in an operational network, adversaries may seek access to critical and sensitive data stores in order to gain an advantage in market transactions, or to disrupt business activities.

Reputational Risk

The financial system depends on trust. For example, if a breach at a bank results in the release of personal data, customers may be reluctant to continue their relationship with the bank. They may choose to pull their deposits out from the bank and close their account. Without trust that customers' money and personal data are safe, the financial system cannot operate smoothly. The Equifax breach illustrates an example where 145 million customers' data was exposed. As a result, the Government Accountability Office (GAO) advised agencies to not use knowledge-based questions (a service which Equifax provided in addition to credit reporting) to authenticate users. Additionally, while customers may not be able to withhold information from Equifax and other credit bureaus, they may become reticent about using financial services if they know their information will be shared with institutions susceptible to similar breaches.

Systemic Risk

Financial institutions are highly interconnected, and many institutions depend on a few widely-accepted systems. Because an attack on one of these IT systems could result in significant losses across the entire industry, financial regulators must also consider the systemic risks to the entire industry. In doing so, they seek to ensure the safety and soundness of not only individual organizations, but also their partners. Systemic risk may have increased in 2020, as the pandemic has increased reliance on technology (e.g., remote payment systems). The Financial Stability Oversight Council (FSOC) has identified three channels through which a cybersecurity event could threaten the stability of the U.S. financial system:

- An incident could disrupt a key financial service or a financial market utility for which there are few substitutes (e.g., the central bank, exchanges, and payment clearing and settlement institutions);
- An incident could cause a loss of confidence among a broad set of customers or market participants; and
- An incident could compromise the integrity of critical data (e.g., altering balance sheets), rendering information critical to financial firms either inaccurate or unusable.

Security Approaches

Laws, regulations, agency authorities, and private sector actions combine to mitigate cybersecurity risks.

Key Laws

Four primary laws make up the statutory framework upon which financial institutions' cybersecurity is based. Although these laws rarely mention cybersecurity specifically, their requirements broadly apply, regardless of the medium on which the information is stored (e.g., on paper or a hard drive), or how it is processed (e.g., by hand or by a computer).

- Gramm-Leach-Bliley Act
- Sarbanes-Oxley Act of 2002
- Dodd-Frank Wall Street Reform and Consumer Protection Act

- The Bank Protection Act

Key Agencies

The Federal Reserve System (the Fed), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), along with representatives from state supervising organizations, comprise the Federal Financial Institutions Examination Council (FFIEC).

The FFIEC IT Handbook provides the standards that financial institutions must abide by for the safety and soundness of the financial system.

Other federal agencies provide guidance or rules to improve cybersecurity, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC).

With so many agencies involved with the cybersecurity of financial institutions, GAO has raised concerns over interagency cooperation and tracking the success of agency efforts.

Key Private Sector Entities

The financial institutions have also organized to bolster the financial system's cybersecurity. Some of these organizations include the Financial Services Sector Coordinating Council (FSSCC), Payment Card Industry Security Standard Council, and the Financial Services Information Sharing and Analysis Center (FS ISAC).

Self-regulatory organizations (SROs), such as the Financial Industry Regulatory Authority (FINRA) for brokers and dealers of securities, provide information security practices and operational controls for their member organizations.

Cross-Cutting Issues in Cybersecurity

This CRS Insight is one of a series on cross-cutting issues in cybersecurity. For others in the series please visit our website. As with others in this series, a podcast accompanies this product. You may access this podcast and others online.

Further Reading

Cybersecurity: An Introduction, by Chris Jaikaran

Fintech: Overview of Innovative Financial Technology and Selected Policy Issues, coordinated by David Perkins

Consumer Data Security and the Credit Bureaus, by Chris Jaikaran

Financial Services and Cybersecurity: The Federal Role, by Maureen Murphy and Andrew Scott

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Andrew P. Scott
Analyst in Financial Economics

Disclaimer