Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

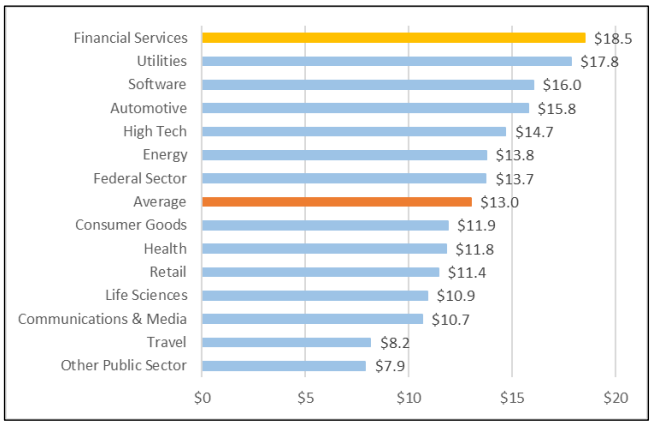
Updated January 13, 2022

Introduction to Financial Services: Financial Cybersecurity

Cybersecurity is a major concern of financial institutions and federal financial regulators. Recent data breaches at large financial institutions have increased concerns about the privacy and security of consumer financial information. For example, in 2019, insurance company First American Financial experienced a breach that exposed 885 million files, including Social Security Numbers and driver's license and account information.

Financial institutions seek to prevent electronic theft of money and other assets, as cyberspace disruptions, such as denial-of-service attacks, could interrupt or shut down their businesses. According to a private study, the per-company cost of cybercrime is over $18 million for financial services companies, around 40% higher than the average cost for other sectors, as illustrated in **Figure 1**.

Figure 1. Costs of Cybercrime Across Sectors
by sector, $ in millions



Source: Figure created by CRS, adapted from Accenture, *Unlocking the Value of Improved Cybersecurity Protection*, July 15, 2019.

Cybersecurity threats pose *operational risk* and *reputational risk*. Operational risk is the threat that an event—such as a natural disaster, pandemic, or cyberattack—limits or completely obstructs an institution's ability to do business. Reputational risk is the threat that customers will take their business elsewhere based on the actions of or associated with a financial institution. For example, if a financial institution fails to secure a customer's information during a cyberattack, the customer may lose trust in the institution. Cybersecurity is a way to protect against some aspects of operational and reputational risk.

If the entire system fails to adequately address cybersecurity concerns, this could lead to *systemic risk*—the risk that a cybersecurity incident would destabilize the financial system. For example, in a highly interconnected financial system, a cybersecurity incident at one of the major banks or payment networks could adversely affect operations at many other financial institutions. 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:

1. 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).
2. An incident could cause a loss of confidence among a broad set of customers or market participants.
3. An incident could compromise the integrity of critical data, rendering information critical to financial firms either inaccurate or unusable.

Further, FSOC's 2020 Annual Report notes that systemic risk may have increased as the COVID-19 pandemic has increased reliance on technology, such as remote payment systems.

Federal Policy Approaches

The federal government has increasingly recognized the importance of cybersecurity in the financial services industry, and federal financial regulators each have a role in cybersecurity. Numerous laws cover aspects of cybersecurity for different industries. Some of these laws contain specific provisions that require financial regulators to implement rules that establish cybersecurity standards for financial institutions, and they provide regulators the authority to supervise these institutions for compliance with such standards. Other laws provide broad authority to regulators to regulate and supervise financial institutions for safety and soundness. Financial regulators rely on these broad authorities to shape cybersecurity policies for the institutions they regulate.

The **Gramm-Leach-Bliley Act of 1999** (GLBA; P.L. 106-102) is the most comprehensive of these laws and directs financial regulators to implement disclosure requirements and security measures to safeguard private information. GLBA provides a framework for regulating data privacy and security practices for financial institutions. This framework is built upon two pillars: (1) privacy standards that impose disclosure limitations on financial institutions concerning consumers' information and (2) security standards that require institutions to implement certain practices to safeguard information from unauthorized access, use, and disclosure. The rules implementing this framework are known as the Privacy Rule (Regulation P) and the Safeguards Rule.

The **Sarbanes-Oxley Act of 2002** (P.L. 107-204) contains provisions requiring a corporation that files reports under

Sections 13(a) and 15(d) of the Securities Exchange Act of 1934 to also file annual reports with the Securities and Exchange Commission that identify internal and external risks to the business and the ways that the company guards against those risks. Bank and thrift holding companies and insured depositories are required to file similar reports with their regulators.

The **Fair and Accurate Credit Transactions Act** (P.L. 108-159) amended the Fair Credit Reporting Act to require regulatory agencies to develop identity theft guidelines, which outline "patterns, practices, and specific forms of activity that indicate the possible existence of identity theft" (15 U.S.C. §1681).

The **Bank Protection Act** (P.L. 90-389), as amended, directs the federal bank regulators to establish minimum security standards for banks and savings associations to "discourage robberies, burglaries, and larcenies" (12 U.S.C. §§1881-1884). Although the law does not mention cybersecurity, bank regulators interpret it to include protection against cyber threats.

Other federal laws, such as the **Bank Service Company Act of 1962** (P.L. 87-856) and the laws that establish the authorities for financial regulators to conduct safety and soundness examinations, allow regulators to regulate and supervise financial institution activities and partnerships (e.g., with technology service providers). Regulators rely on these broad authorities to shape and impose cybersecurity on the institutions they regulate. For example, the banking regulators monitor cybersecurity issues by conducting on-site examinations under their authority to examine banks for safety and soundness and can require banks to take remedial action if their cybersecurity policies are deficient. Further, in November 2021, the banking agencies implemented new requirements for financial institutions to notify their primary regulators within 36 hours of a cybersecurity incident and for bank service providers to notify any affected banks as soon as possible. Additionally, the Federal Financial Institutions Examination Council (FFIEC) has developed the Cybersecurity Assessment Tool to help institutions identify their risks and determine their cybersecurity preparedness.

Policy Considerations for Congress

Oversight of financial services and bank cybersecurity reflects a complex and sometimes overlapping array of state and federal laws, regulators, regulations, and guidance—many of which predate the emergence of cybersecurity risk. Whether this framework is effective and efficient, resulting in adequate protection against cyberattacks without imposing undue cost burdens on banks, is an open question. The occurrence of successful hacks of banks and other financial institutions, wherein huge amounts of personal information are stolen or compromised, highlights the importance of ensuring bank cybersecurity. Further, the fact that several regulators implement, supervise, and enforce federal provisions has raised questions over the patchwork of regulatory standards for consumer privacy and security. Some argue that a unified and modernized legislative framework could improve this patchwork approach.

Other policy considerations for Congress are listed below.

Data Security Standards

One area of debate is whether data security standards should be prescriptive and government-defined or flexible and outcome-based. Some argue that a prescriptive approach could be inflexible and harm innovation; others argue that an outcome-based approach might lead to institutions having to comply with a wide range of data standards. For instance, in October 2021, the Federal Trade Commission (FTC) issued a rule that updates the Safeguards Rule with more specific criteria for what financial institutions must implement.

Financial Data and Consumer Redress

GLBA covers only nonpublic personal information held by financial institutions significantly engaged in financial activities. As the industry's data use has grown, some have debated whether the law covers all sensitive individual financial information. For example, data brokers can compile public and private data from different sources. Much of these data may not be subject to GLBA's provision, but combining them might reveal sensitive information about a consumer. Further, consumers have a limited ability to control or correct financial data, which can make it difficult to obtain redress for data breaches.

Vendors, Cloud Providers, and Systemic Risk

Banks pay cloud service providers (CSPs) to use CSPs' computing resources (e.g., servers) rather than maintaining their own. Use of CSPs can be emblematic of banks' relationships with a broader base of vendors and how these ties may introduce more cybersecurity risks. Cyber risks change, and may increase, for banks with increased reliance on advanced IT solutions, such as cloud. Also, many banks rely on a few providers (three major CSPs account for 60%-70% of market share), and this could transform cyber risk to systemic risk, with FSOC noting that a "cyber event at a critical vendor with a large number of clients could result in widespread disruption in access to financial data and could impair the flow of financial transactions." Concentration risk and operational concerns, such as lock-in risk, may bias banks toward multi-cloud strategies—contracts with and technology postures consisting of multiple CSPs—thereby expanding the relationships for which banks must manage cybersecurity.

CRS Resources

CRS Report R44429, *Financial Services and Cybersecurity: The Federal Role*, by M. Maureen Murphy and Andrew P. Scott

CRS Insight IN11199, *Big Data in Financial Services: Privacy and Security Regulation*, by Andrew P. Scott

CRS Testimony TE10021, *Consumer Data Security and the Credit Bureaus*, by Chris Jaikaran

CRS In Focus IF11985, *Bank Use of Cloud Technology*, by Paul Tierno

Andrew P. Scott, Analyst in Financial Economics
Paul Tierno, Analyst in Financial Economics

Disclaimer