2024 Report on Cybersecurity and Resilience

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Table of Contents –

software include disclosure of credentials or confidential data, corruption of data, installation of malware, and application outages. These problems can result in lost time, money, and customer trust. IBM's Cost of a Data Breach Report 2023[78] reflected that 15 percent of organizations identified a supply chain compromise, and 12 percent identified a software supply chain attack, as the source of a data breach.

An example of a supply chain threat that plagued the financial sector was the compromise by Russian-based Cl0p ransomware group of a since-patched vulnerability in a widely used file transfer application software called MOVEIt. The MOVEIt campaign targeted the U.S. financial sector and other enterprises globally with estimates of 2,618 organizations and 77 million individuals affected.

Strategic

Strategic cybersecurity threats are those that are more likely to result in disruptions in the long-term but require current preparation and planning to prevent disruption and add resilience. For example, malicious actors are leveraging generative artificial intelligence (AI) technologies to circumvent identity- and authentication-based financial institution network defenses and to perpetrate other frauds. These perpetrators of financial crimes are increasingly using AI to create fraudulent or altered documentation, audio files, and video recordings, leading to increasing number of fraud cases.[79] The pervasiveness of generative AI tools allow malicious actors to easily leverage the technology to create more convincing or realistic content or materials to further fraud schemes.[80] Generative AI, including large language models, can augment live videos via "deepfakes" or voice cloning tools, making it more difficult for financial institutions to discern real versus fraudulent (including synthetic) identities during customer account opening, processing of transactions, or verification processes.

Another example of a strategic cybersecurity threat is the continuing development of quantum computing technology. Quantum computers use a different computing architecture that can solve certain types of problems much faster, including some encryption algorithms. Once fully developed, it is anticipated that quantum computing will provide substantially greater computing speed and power, as compared to current models. Quantum computing is expected to eventually weaken or incapacitate the current encryption methods that the financial sector uses to secure the integrity and confidentiality of its networks and data against cyber attackers.

Conclusion

The FDIC appreciates the opportunity to provide this report on the FDIC's efforts to address cybersecurity threats and its efforts in partnership with other private and public sector stakeholders.

[78] IBM, "Cost of a Data Breach Report 2023," December 2023.
[79] Sift, "Q2 2023 Digital Trust & Safety Index – Fighting Fraud in the Age of AI and Automation," June 22, 2023.
[80] Precedence Research, "Generative AI Market Growth Is Booming With 27.02%," July 11, 2023.