PUBLICATION

Cybersecurity Preparedness: Standardization is Key

Authors: Matthew George White
August 2019

On August 28, 2019, the Federal Financial Institutions Examination Council (FFIEC) issued a press release encouraging organizations to utilize a standardized approach to assess and improve cybersecurity preparedness. The release emphasized that organizations adopting a standardized approach are better able to track their progress over time and share information and best practices with other financial institutions and regulators.

While organizations may choose from a variety of standardized tools aligned with industry standards and best practices, the FFIEC directed organizations to several tools to assist in developing a standardized approach. Links to each of these tools, as well as a brief description of each, are included below:

- FFIEC Cybersecurity Assessment Tool – Developed by the FFIEC, the Assessment provides a repeatable and measured process for financial institutions to identify their risks and determine their cybersecurity preparedness. The Assessment includes a five-step process flow incorporating review of pertinent information, guided self-assessment, and review and evaluation of the results. The Assessment is intended to be consistent with the FFIEC Information Technology Examination Handbook, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and industry accepted cybersecurity practices.

- FSSCC Cybersecurity Profile – Developed by the Financial Services Sector Coordinating Council (FSSCC), the Profile is a scalable and repeatable assessment that financial institutions can use for internal and external *(i.e.*, third party) cyber risk management assessment. The self-assessment in the Profile requires diagnostic statements regarding several overarching functions: governance, identify, detect, protect, respond, recover and supply chain/dependency management. It then provides a mechanism for organizations to identify and implement a plan to close any gaps. The Profile is based on the NIST Framework for Improving Critical Infrastructure Security, CPMI-IOSCO's Guidance on Cyber Resilience for Financial Market Structures, supervisory guidance and frameworks, and direct correlative mappings to ISO/IEC 27001/2 controls.

- NIST Cybersecurity Framework – Created through collaboration between industry and government, this voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. It is intended to be a prioritized, flexible, repeatable, and cost-effective approach to assist owners and operators of critical infrastructure to manage cybersecurity-related risk. The Framework consists of three main components: the Core, Implementation Tiers, and Profiles. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes. The Framework Implementation Tiers assist organizations by providing context on how an organization views cybersecurity risk management. Framework Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core.

- Center for Internet Security Controls – The CIS Controls are intended to be used by IT security leaders to quickly establish the most significant protections for their organizations. The Controls guide organizations through a series of 20 foundational and advanced cybersecurity actions, intended to eliminate the most common cybersecurity attacks.

While the FFIEC encouraged the use of these tools, it reminded organizations that no specific tools are endorsed by the FFIEC and will not take the place of the risk-focused examinations to which members are subject. The FFIEC specifically noted that as cyber risk evolves, examiners may address areas not covered by these tools.

If you have any questions regarding developing or implementing a standardized approach to your cybersecurity preparedness efforts, or if you need assistance with any other cybersecurity or data privacy-related matters, please contact Matt White, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.