Lowenstein Sandler

Client Alert

Data, Privacy & Cybersecurity

March 6, 2024

NIST Releases Cybersecurity Framework 2.0

By Amy S. Mushahwar, P. "Kai" Knight, and Waleey Fatai

The National Institute of Science and Technology (NIST) has released NIST Cybersecurity Framework (2.0) (Framework 2.0). NIST released two earlier versions of the Framework for Improving Critical Infrastructure Cybersecurity in 2014 and 2018, designed to put cybersecurity controls in a more functional framework to understand risk and focus cybersecurity efforts.

Framework 2.0 provides guidance to industry, government agencies, and other organizations on how to efficiently manage cybersecurity risks. It organizes cyber control areas into core functions that organizations should aim to have in place in their overall cybersecurity processes: Identify; Protect; Detect; Respond; and Recover. All five were in the older versions of the standard and Framework 2.0 has ushered in a new core function, Govern, identifying that cybersecurity is a key enterprise risk to be managed. Increased focus on cyber enterprise risk governance is a key theme we have seen echoed by other regulators, including the Securities and Exchange Commission, Federal Trade Commission, and New York Department of Financial Services.

Below, we briefly outline each of these core areas, starting with the newest function, Govern.

GOVERN

The Govern function defines an organization's overall risk management strategy and expectations and includes policy establishment, management, and monitoring. Organizations should understand their own organizational contexts and devise cybersecurity and supply chain risk management strategies that work for their specific circumstances. It may not be best for an organization to simply adopt the cybersecurity processes used by peer organizations, because no two organizations will have the exact same set of cybersecurity circumstances or management style.

IDENTIFY

Beyond establishing a general cybersecurity regime, an organization should study and understand its own cybersecurity vulnerabilities, including its data, hardware, systems, services, people, etc. For example, an organization that processes individuals' sensitive personal information with a third-party vendor as part of its core business would have a different risk assessment than one that simply sells tangible goods. Understanding its own risks and vulnerabilities enables that organization to prioritize its efforts consistent with its mission needs and risk management strategy.

PROTECT

Once the risks and vulnerabilities are identified, the organization should consider its means of securing its assets and minimizing the likelihood and/or impact of cybersecurity events. Specific action plans here could include authentication, access control, data and platform security, and training.

DETECT

In the unfortunate instance of a cybersecurity attack, an organization wants to be well positioned to quickly detect the attack and determine points of compromise. Essentially, organizations should have an incident response system in place.

RESPOND

And to further protect itself, an organization should respond in a way to ensure that the impacts of any attacks are mitigated. This function also includes making any required compliance reporting and/or communication.

RECOVER

In responding to a cybersecurity incident, an organization should have a system in place to restore its normal operations to reduce the effects of that incident on its overall business objectives or outlook.

Framework 2.0 suggests that the Govern, Identify, Protect, and Detect functions be run simultaneously, while the Respond and Recover functions should be ready to address any cybersecurity incidents.

In releasing the new standard, NIST created very helpful Quick Start Guides that organizations may use to track their understanding, assessment, prioritization, and communication of the key functions described above. Specifically, there are organizational profiles with implementation considerations including small-business resources, technology acquisition guidance, and enterprise risk management support, among other items on the Quick Start Guide page. NIST spent considerable time developing resources to help speed implementation of Framework 2.0 and prioritize risk, in addition to simply updating its text, including a very handy FAQ page at https://www.nist.gov/faqs.

For further information on how to implement Framework 2.0, please reach out to any of the authors of this alert.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data, Privacy & Cybersecurity
T: 202.753.3825
amushahwar@lowenstein.com

P. "KAI" KNIGHT
Counsel
T: 202.753.3828
kknight@lowenstein.com

WALEEY FATAI
Associate
T: 212.419.6040
wfatai@lowenstein.com