JENNER & BLOCK

NIST Cybersecurity Framework 2.0 Released

Client Alerts

March 5, 2024
By: Madeleine Findley, Shoba Pillay

On February 26, 2024, the National Institute of Standards and Technology (NIST), an agency within the U.S. Department of Commerce, released Version 2.0 of its Cybersecurity Framework (CSF), the first major update since its 2014 release.[1] Version 2.0 emphasizes the importance of governance by adding a sixth Core Function to the framework. In addition, Version 2.0 expands the CSF beyond critical infrastructure, promotes secure supply chains, and includes a new suite of additional guidance to assist with implementation.

NIST: A Standard for Managing Cybersecurity Risk

The NIST CSF is the landmark guidance on reducing cybersecurity risk. It was released as part of a broader federal initiative to improve cybersecurity and has served as benchmark for large companies and organizations since it was first published. It aims to help organizations understand, reduce, and communicate about cybersecurity risk.

While the NIST CSF may be adopted voluntarily, it has been incorporated into government policies and mandates both within and outside the United States. Companies regularly use the NIST CSF to navigate complex and overlapping cybersecurity regulatory regimes. By way of illustration, Connecticut and Ohio's data breach statutes provide safe harbors to companies that follow the NIST CSF.

It is important to note that it is challenging for any company to reach total compliance with the NIST CSF. Instead, the NIST CSF is an aspirational maturity model. Companies that inaccurately boast full compliance with the NIST CSF could face regulatory scrutiny. For instance, self-reported compliance with the NIST CSF is key evidence in the SEC's enforcement action against SolarWinds.

Version 2.0: Accessible and Modernized

Before last week, the NIST CSF had not been substantially updated since 2014. Version 2.0 supports the White House's National Cybersecurity Strategy and is the culmination of years of coordination with stakeholders and industry players. It offers a robust, workable framework that expands the CSF's guidance on managing cybersecurity risk.

Key updates in Version 2.0 target governance, expansion beyond critical infrastructure, and supply chain vulnerabilities.

Adding An Emphasis On Governance

CSF version 1.0 was organized around five key functions that parallel the life cycle of managing cybersecurity risk: identify, protect, detect, respond, and recover. These functions are divided into categories and subcategories that offer granular guidance on CSF's recommendations. Version 2.0 adds a sixth overarching function: "govern." The "govern" function provides outcomes to inform what an organization can do to achieve and prioritize the previous five functions in the context of its mission and stakeholder expectations. These initiatives target the organization's stakeholders and decisionmakers to make sure they are invested in and foster accountability regarding cybersecurity risk assessment and compliance.

This added emphasis on governance targets the development and execution of organizations' cybersecurity strategy. Version 2.0 emphasizes cybersecurity as a major source of risk that senior leadership must consider along with traditional risks such as financial, supply chain, reputational, and physical. Buy-in from senior leadership is essential and must be communicated throughout the organization.

Accessibility for Entities Beyond Critical Infrastructure

While Version 1.0 focused on critical infrastructure such as hospitals and power plants, Version 2.0 addresses a broad array of sectors, including industry, nonprofit organizations, schools, and local government entities—regardless of their level of cybersecurity sophistication.

To help these organizations navigate their cybersecurity risk, Version 2.0 is accompanied by a suite of resources designed to meet these entities where they are and help them navigate and implement the framework. These online resources complement the NIST CSF and include a community page to learn from other users' success stories, quick-start guides designed for specific industries and users such as small businesses and enterprise risk managers, and a reference tool to simplify applying the NIST CSF. Organizational profiles on the NIST website will help organizations compare where they are versus where they could be depending on their size and industry. Version 2.0 describes desirable outcomes but does not prescribe these outcomes or how they can be achieved. The "how" is available via these online tools.

Supply Chain Risk Management

Version 2.0 addresses the reality that cybersecurity supply chains rely on complex, global, and interconnected supply chains with multiple levels of outsourcing between public and private entities. Supply chain risk management is thus a critical part of every organization's cybersecurity risk planning. Version 2.0 includes supply chain risk management guidelines in the cybersecurity and governance function (G-SCRM). NIST also released a related guide on supply chain risk management in 2022.

Conclusion

Version 2.0 of the NIST CSF ushers in a more broadly applicable and tailored framework to manage cybersecurity risk. Its expansion into industries beyond critical infrastructure render it more applicable across industries and organizational structures, and may lead to a heightened expectation that organizations at all levels of cybersecurity sophistication implement its guidelines.

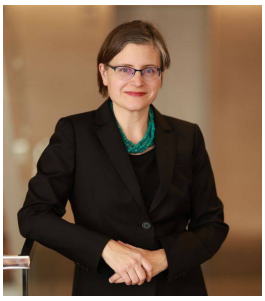
With regulations in the works requiring audits of organizations' cybersecurity programs, bringing cyber policies into line with NIST CSF may assist in avoiding regulatory scrutiny.[2] Jenner & Block stands ready to assist clients in developing robust cybersecurity programs using a compliance, risk, and governance model.

Footnotes

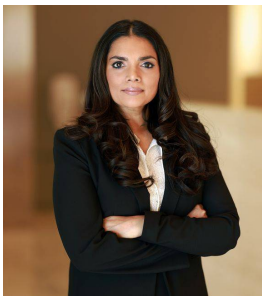
[1] https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10.

[2] *See, e.g.*, Client Alert: California Privacy Protection Agency Releases Initial Draft Proposed Rules for Risk Assessments and Cybersecurity Audits, https://www.jenner.com/en/news-insights/publications/client-alert-california-privacy-protection-agency-releases-initial-draft-proposed-rules-for-risk-assessments-and-cybersecurity-audits.

Related Attorneys



Madeleine Findley
Partner
mfindley@jenner.com
+1 202 639 6095



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →