MAYER • BROWN

Legal Update
February 22, 2017

NIST Releases Updated Cybersecurity Framework and Guide for Cybersecurity Event Recovery

Three years ago, the National Institute of Standards and Technology ("NIST") released the "Framework for Improving Critical Infrastructure Cybersecurity." In the intervening years, NIST and numerous other US government departments and agencies have continued to release guidance on how to improve cybersecurity using a tailored risk management framework. In recent months, NIST has continued this trend. In December 2016, NIST released a new guide for "Cybersecurity Event Recovery" (SP 800-184), and in January 2017, NIST published the draft "Framework for Improving Critical Infrastructure Cybersecurity v. 1.1." Each issuance reflects NIST's focus on developing risk-based approaches for protecting against cyber attacks. Below we outline the guidance and key implications for businesses.

NIST Cybersecurity Framework

Since its release, the Framework has been widely adopted by companies in a broad range of industries. The updates to the Framework released in January retain the basic structure of the original document and its focus "on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes." While these updates make a limited set of changes, they have the potential to augment the Framework's utility for private sector entities, particularly in their emphasis on cyber supply chain risk management and the use of cybersecurity metrics.

BACKGROUND

On February 12, 2014, NIST released a "Framework for Improving Critical Infrastructure Cybersecurity v. 1.0," in response to President Obama's Executive Order 13636. (See our update on the original Framework.) Now widely used by companies across industries, the Framework provides "a common taxonomy and mechanism for organizations to: 1) Describe their current cybersecurity posture; 2) Describe their target state for cybersecurity; 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; 4) Assess progress toward the target state; [and] 5) Communicate among internal and external stakeholders about cybersecurity risk."

Framework Version 1.0 consisted of three parts: the Core, Implementation Tiers and Profile. Most significantly, the Framework Core identified five primary cybersecurity functions: Identify, Protect, Detect, Respond and Recover. Each function had multiple corresponding categories, subcategories, and informative references. This structure thus described five broadly accepted cybersecurity focus areas and then presented detailed activities that organizations could undertake in each area.

VERSION 1.1

On January 10, 2017, NIST released a "draft update" to the Framework that is intended to clarify aspects of the original version, provide new suggestions on managing cyber supply chain risks, and introduce measurement methods for cybersecurity, among other changes. These developments respond to feedback received from industry stakeholders through formal comments, frequently asked questions and a public workshop.

Stakeholders will have an opportunity to submit comments on the updated draft until April 10, 2017, and to participate in a public workshop in May. NIST will also be hosting webinars on March 1 that will provide more information on the proposed updates. Currently, NIST expects to produce a final version of the draft by fall 2017.

Although Version 1.1 adopts the same basic approach taken in Version 1.0, NIST has made several notable changes in this draft, particularly with respect to: cybersecurity measurement and supply chain risk management. Below, we discuss these and other changes.

CYBERSECURITY MEASUREMENT

Version 1.1 of the Framework adds a new section 4.0, *Measuring and Demonstrating Cybersecurity*, which provides an overview of how the Framework can be used to measure cybersecurity outcomes and trends. Measuring cybersecurity facilitates the conveyance of "meaningful risk information" that can inform business decision-making. Tracking cybersecurity metrics can help an organization evaluate its overall risk posture and even reveal "how changes in granular security controls impact the completion of business objectives." Organizations can gain value from measuring cybersecurity by correlating cyber improvements with business results.

The Framework suggests how an enterprise could use the outcomes identified in the Framework Core as the basis for measurement and subsequently accountability for cybersecurity performance. Relatedly, the new section also ties specific cybersecurity measurements to elements of the Framework.

SUPPLY CHAIN RISK MANAGEMENT

In recent years, stakeholders both in government and the private sector have coalesced around the importance of appropriate supply chain risk management in cybersecurity. When the Framework was originally released, the accompanying Roadmap outlining areas for continued improvement identified supply chain risk management as "an essential part of the risk landscape." The recent updates incorporate this concern throughout the Framework.

For example, the Framework Implementation Tiers now include cyber supply chain risk as an element of Tier selection. Thus, while an organization at Tier 1 "may not understand the full implications of cyber supply chain risks," an organization at Tier 4 "can quickly and efficiently account for emerging cyber supply chain risks using real-time or near real-time information and leveraging an institutionalized knowledge of cyber supply chain risk management with its external suppliers and partners as well as internally." In addressing how cybersecurity requirements are conveyed to stakeholders, the Framework also suggests that entities consider "[e]nacting cybersecurity requirements through formal agreement" and "[c]ommunicating to suppliers and partners how those cybersecurity requirements will be verified and validated." Finally, the new focus on supply chain risk is also reflected in a new category in the Framework Core recommending that an organization establish processes to "identify, assess and manage supply chain risks."

OTHER DEVELOPMENTS

The updated Framework includes other changes that help to clarify how the Framework functions and that address specific areas of concern. For example, the revisions incorporate additional focus on authentication, authorization and identity proofing through changes to a provision on access control. The Framework also clarifies the relationship between Implementation Tiers and Profiles, stating that "[t]he risk disposition expressed in a desired Tier should influence prioritization within a Target Profile."

Guide for Cybersecurity Event Recovery

In the wake of significant cybersecurity incidents in both the public and private sectors, stakeholders have focused extensively on improving cybersecurity incident *response* capabilities. In December 2016, NIST complemented this existing emphasis by releasing new guidance that recognizes—consistent with the understanding of private sector stakeholders—the importance of incident *recovery* (which, like "response," is one of the five functions in the NIST Framework). Special Publication 800-184, *Guide for Cybersecurity Event Recovery*, emphasizes the centrality of "recovery" in effective and successful enterprise cybersecurity and "provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning." This is the first federal guide to focus "solely on improving cybersecurity recovery capabilities." This guidance may prove valuable as organizations work to ensure that both response and recovery activities are incorporated in plans, policies and procedures that address cybersecurity incidents.

The purpose of the guide is "to support organizations in a technology-neutral way in improving their cyber event recovery plans, processes, and procedures, with the goal of resuming normal operations more quickly." The guide "is not an operational playbook," but rather "provides guidance to help organizations plan and prepare recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plans." While the document is directed at US federal agencies, it provides valuable information to any organization seeking to refine recovery processes.

The guide is divided into several sections that address planning for recovery, continuously improving recovery processes, identifying metrics to evaluate recovery and creating a recovery "playbook."

PLANNING FOR CYBER EVENT RECOVERY

The guide explains that "[e]ffective planning is a critical component of an organization's preparedness for cyber event recovery." Planning enables an organization to identify vulnerable systems, designate the personnel responsible for protecting them, arrange for adequate resourcing and staffing in the event of an incident and contribute generally to business continuity objectives. The guide makes several "key recommendations" for planning processes, including:

- "Understand how to be prepared for resilience at all times, planning how to operate in a diminished capacity or restore services over time based on their relative priorities."
- "Identify and document the key personnel who will be responsible for defining recovery criteria and associated plans, and ensure these personnel understand their roles and responsibilities."
- "Develop comprehensive plan(s) for recovery that support the prioritizations and recovery objectives, and use the plans as the basis of developing recovery processes and procedures that ensure timely restoration of systems and other assets affected by future cyber events."
- "Formally define and document the conditions under which the recovery plan is to be invoked, who has the authority to invoke

the plan, and how recovery personnel will be notified of the need for recovery activities to be performed."

- "Develop a comprehensive recovery communications plan, and fully integrate communications considerations into recovery policies, plans, processes, and procedures."

CONTINUOUS IMPROVEMENT

The guide also recommends that entities engage in a process of continuously improving their plans and policy documents "by addressing lessons learned during recovery efforts and by periodically validating the recovery capabilities themselves." The guide makes several "key recommendations" for such improvements, including:

- "Formally implement cyber event recovery exercises and tests at a frequency that makes sense for the organization, recording the results to help inform organizational cybersecurity activities."
- "Conduct comprehensive post exercise debriefs to ensure the organization analyzes and incorporates lessons learned into the related plans and processes."
- "Continually improve cyber event recovery plans, policies, and procedures by addressing lessons learned during recovery efforts and by periodically validating the recovery capabilities themselves."
- "Use recovery as a mechanism for identifying weaknesses in the organization's technologies, processes, and people that should be addressed to improve the organization's security posture and the ability to meet its mission."
- "At a minimum, validate recovery capabilities by soliciting input from individuals with recovery responsibilities and conducting exercises and tests."

RECOVERY METRICS

The guide, like the updated Framework, also recognizes the value in identifying appropriate metrics to assess and help improve recovery plans and processes. However, the guide emphasizes that this task is secondary to the goal of "restoring business functions" and counsels that a focus on metrics should not distract from or "create additional obstacles for recovery team efficiency." While acknowledging such concerns, metrics can also "improve specific aspects" of recovery efforts, support "a cost/benefit analysis of a particular approach," provide information for required reporting or enable information sharing. The guide provides a table identifying relevant "Recovery Areas" and corresponding metrics. For example, to measure the "Quality of Recovery Activities," it suggests evaluating metrics like the "[n]umber of business disruptions due to IT service incidents," or the "[p]ercent of successful and timely restoration from backup or alternate media copies."

BUILDING THE PLAYBOOK

The guide defines a "playbook" as "an action plan that documents an actionable set of steps an organization can follow to successfully recover from a cyber event." The guide recommends that a playbook be tailored to an organization's assets and outline actions for achieving a successful recovery. The guide differentiates between two phases of recovery actions: tactical and strategic.

In the tactical phase of recovery, the organization executes the playbook it developed during the planning stage and focuses on the "initiation, execution and termination" of recovery efforts. By contrast, the strategic phase emphasizes activities that focus on the continuous improvement of those same recovery efforts and the "risk management process lifecycle driven by the recovery activities." The guide provides examples of activity in each phase, drawing from many of the recommendations it had already identified. The section concludes by noting that "[t]hese actions are general recommendations that can be tailored in order to fit each organization's specific requirements."

EXAMPLE SCENARIOS

The final two sections of the guide provide examples of how to apply the recovery principles outlined in the document to different cybersecurity incidents. "Section 6 provides an example of a data breach cyber event recovery scenario," while Section 7 provides similar information in the context of a "ransomware event recovery scenario." Each example identifies necessary "pre-conditions" for a successful recovery and actions to be taken at the tactical and strategic phases of recovery.

Conclusion

The extensive adoption of the Framework across industries reflects the broad recognition that risk-based, enterprise-wide approaches are most successful in addressing cyber threats. The decision not to change the core elements of the Framework in version 1.1 should encourage companies to continue to develop and refine such cybersecurity programs within their enterprises, while drawing on the updates to the Framework and the new recovery guidance. As threats continue to grow in scale and complexity, these new documents ultimately reiterate that companies still should base their cybersecurity programs in sound risk-management principles, implemented in a manner that is tailored to the specific systems and data that a company holds and the threats it faces.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

Marcus A. Christian
+1 202 263 3731
mchristian@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Kendall C. Burman
+1 202 263 3210
kburman@mayerbrown.com

Joshua M. Silverstein
+1 202 263 3208
jsilverstein@mayerbrown.com

Mayer Brown is a global legal services organization advising many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, CAC 40, DAX, Hang Seng and Nikkei index companies and more than half of the world's largest banks. Our legal services include banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory & enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit our web site for comprehensive contact information for all Mayer Brown offices. www.mayerbrown.com

Any tax advice expressed above by Mayer Brown LLP was not intended or written to be used, and cannot be used, by any taxpayer to avoid U.S. federal tax penalties. If such advice was written or used to support the promotion or marketing of the matter addressed above, then each offeree should seek advice from an independent tax advisor.

Mayer Brown comprises legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown Mexico, S.C., a sociedad civil formed under the laws of the State of Durango, Mexico; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services.

"Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.