NIST Publishes Suggested Cybersecurity Framework

ADAM SMITH | DATA PRIVACY SOLUTIONS | FEB 14, 2014

On February 14, 2014, the National Institute of Standards and Technology released its long-awaited cybersecurity Framework, which is entitled "Framework for Improving Critical Infrastructure Cybersecurity." The Framework provides best practices for voluntary use in all critical infrastructure sectors, such as financial services, healthcare, government, and transportation.

The Framework came in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which was issued by the President on February 12, 2013. The Order provided that, "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework does this by focusing on three separate areas: The Framework Core, the Framework Profile, and the Framework Implementation Tiers.

The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles.

The Framework Profile is designed to help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.

The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

Notably, implementation of the Framework is not mandatory. Indeed, the Framework acknowledges that different businesses and industries face all kinds of distinct challenges when it comes to cybersecurity. Notwithstanding, companies must be aware that this Framework is available as it may be seen by regulatory agencies as another counteractive measure that companies should have employed or, at the very least, consulted to reduce exposure to a data breach. Said differently, because this is a federal publication derived from a Presidential Executive Order, it would be advisable for organizations to know of the Framework's existence and utilize it as a resource to help install proactive measures to effectively deal with a data breach when it occurs. McDonald Hopkins is a law firm that is equipped to assist organizations with developing such proactive measures. Organizations will, at some point, be the victims of a data breach. The only question will be: how prepared is that organization to deal with the breach?

ADAM SMITH

Read More