Thinking Ahead – Implementing the NIST Cybersecurity Framework to Protect from Potential Legal Liability

by: Markus Rauschecker, J.D.
Senior Law and Policy Analyst, University of Maryland Center for Health and Homeland Security
Adjunct Professor of Law, University of Maryland Francis King Carey School of Law

Private sector organizations should be motivated to implement the NIST Cybersecurity Framework not only to enhance their cybersecurity and to benefit from added incentives to do so, they should also implement the Framework to lower their potential risk of legal liability.

Failure by the U.S. Congress to pass meaningful cybersecurity legislation led the President to act within his power to address the Nation's cybersecurity vulnerabilities. Last year, he issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity. Among other initiatives, the Executive Order called on the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework that provides guidance on common standards and best practices to critical infrastructure organizations for enhancing their cybersecurity.

Unlike legislation, however, the reaches of an Executive Order are more limited. While executive branch agencies must adhere to the Executive Order, private companies and organizations are not required to adopt the Framework. Its implementation is therefore considered voluntary within the private sector. Indeed, the voluntary nature of the Framework was stressed throughout its development and is still highlighted now after its release.

Nonetheless, the Administration obviously wants to encourage the Framework's implementation within any organization. Recognizing the limitations of an

Executive Order, government began working on incentivizing the Framework's adoption. To increase adoption by private entities, certain incentives are being considered, including: implementation of the Framework as a condition of contracting with the government or receiving government grants, preferential insurance rates, receiving technical assistance, public recognition, and more. Once available, these incentives will undoubtedly help get organizations to apply the Framework.

Valuable incentives, however, are not the only reason why a private sector organization will want to implement the Framework within its enterprise. Even if an organization feels confident in its cybersecurity or does not find the available incentives enticing enough, the organization will still want to strongly consider putting the Framework into practice as a way to lower the risk of possible legal liability.

As cyber attacks and data breaches increase, companies and other private organizations will inevitably face lawsuits from clients and customers. When these lawsuits reach the courts, courts will look to identify a standard of care by which those companies or organizations should have acted to prevent harm. If the company or organization failed to live up to the identified standard, it could face legal liability. Given its origins and content, courts may well come to define the Framework as the minimum legal standard of care by which a private sector organization's actions are judged.

The prospect of courts seeing the Framework as the standard of care is especially real since the Framework came out of an extensive collaborative effort by government, the private sector, and academia. Thousands of individuals and organizations were involved in shaping the Framework through their responses to requests for information and national workshops. Moreover, it is important to note that in its final version the Framework does not propose any new standards or practices. It summarizes existing standards and best practices and provides the best consensus on what stakeholders believe to be reasonable and prudent cybersecurity practices. Because the Framework encapsulates current and generally

As cyber attacks and data breaches increase, companies and other private organizations will inevitably face lawsuits from clients and customers.

accepted guidelines by which an organization may strengthen its cybersecurity, courts will likely be very interested in seeing whether a defending organization was acting in accordance with these practices. If courts find that a defending organization was not following the practices contained in the Framework, and if failure to follow those practices caused harm, courts could end up holding the organization legally liable. That could mean huge costs to the organization.

What is more, the Framework not only provides commonly recommended cybersecurity activities by which organizations can become more secure, it also provides the tools for assessing an organization's approach to enforcing cybersecurity. These tools allow an organization to assess its own status against the benchmark that the Framework sets. Inevitably, these tools and assessments will also enable organizations to compare themselves to other organizations. Courts could choose to make the same comparisons and find an organization did not meet the necessary standard of care if it failed to implement the Framework.

Should Congress pass cybersecurity legislation at some point, that legislation may well mandate the implementation of cybersecurity measures within the private sector, address liability issues, and even set

a clear legal standard of care. The hope for smart, effective legislation still exists. Until then, however, organizations should be motivated to integrate the standards and best practices put forth by the Framework into their enterprise. The desire for strong cybersecurity and the proposed incentives should make implementing the Framework well worth the cost. Additionally, the risk of courts finding legal liability for a failure to meet the Framework's standards provides extra motivation to any organization. Ultimately, implementing the Framework is good business sense and makes individual organizations, and the Nation as a whole, more secure.

Mr. Rauschecker received his JD from the University of Maryland, Francis King Carey School of Law in 2006 and is admitted to practice law in the state of Maryland . He joined CHHS in 2008 and has worked on several projects ranging from providing legal and policy analysis for the National Capital Region to program management for the District of Columbia's Presidential Inauguration Committee and lead planner for the District's Continuity of Operations program. He also co-teaches a Law and Policy of Cybersecurity course at the School of Law.

CHHS
CENTER FOR HEALTH & HOMELAND SECURITY