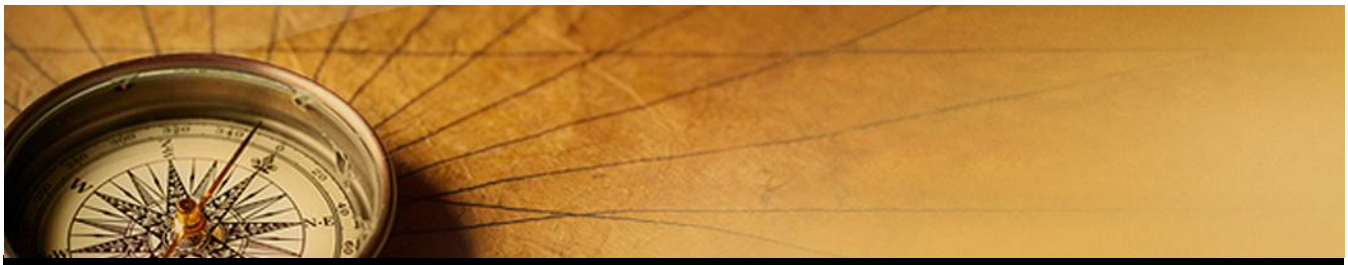

David Leiter, DJLeiter@mlstrategies.com
Jeremy Rabinovitz, JRabinovitz@mlstrategies.com
Bill Weld, BWeld@mlstrategies.com
Mo Cowan, MCowan@mlstrategies.com
Abby Matousek, AMatousek@mlstrategies.com
Rachel Sanford, RMSanford@mlstrategies.com

Follow us on Twitter: @MLStrategies

ML Strategies, LLC
701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004 USA
202 434 7300
202 434 7400 fax
www.mlstrategies.com

The NIST Cybersecurity Framework and Implications for the Financial Services Industry

The NIST Framework

The National Institute of Standards and Technology (NIST) issued a "Framework for Improving Critical Infrastructure Cybersecurity" on February 12th. This set of voluntary best practices for critical infrastructure was developed over the course of the past year based on stakeholder input during a number of open comment periods and stakeholder workshops under President Obama's Cybersecurity Executive Order that was issued in February 2013. As part of the framework, NIST also released a Roadmap discussing next steps and identifying key areas for development, alignment, and collaboration.

For the purposes of the framework and roadmap, critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Now that NIST has released the final framework, it will be up to the Department of Homeland Security to promote the voluntary best practices.

Industry Response

Among those industries considered to be critical infrastructure under the framework is the financial services and banking sector. The framework was largely met with support from the embattled financial services industry, which has been plagued by data security concerns and other forms of cyber-attacks. The framework provides additional clarity and guidance to support private sector steps already being taken to bolster security. For example, in 2013 the financial services industry, led by the Securities Industry and Financial Markets Association (SIFMA), conducted "Quantum Dawn 2," an exercise that simulated a systemic cyber-attack across fifty participants, including banks, exchanges, regulators, and federal law enforcement.

The NIST framework builds on this private sector effort by providing banking and financial institutions with a means of measuring institutional security standards against federal guidelines. In addition to providing additional guidance on how to prepare and combat risks, the framework is intended to better enable the financial industry to balance its preventative measures and response with its appetite for risk and resources to combat cyber threats. The Treasury Department also praised the guidelines, emphasizing that

the risk-based approach to managing cybersecurity will allow larger firms with existing cyber standards to refocus on best practices and enable small institutions to "better understand their risk profile and establish protocols for ensuring proper controls are in place to meet that profile."

However, while the response to the framework was generally positive, banks already dealing with the continued implementation of Dodd-Frank Act regulatory reforms fear that the NIST standards could be a stepping stone to increased regulation and additional compliance costs. For example, the National Association of Federal Credit Unions praised the standards but reminded regulators that credit unions and other institutions are "already subject to stringent regulatory requirements under the Gramm-Leach-Bliley Act" and continually work to make cybersecurity a priority.

Legislative and Regulatory Outlook

While the framework has been met positively by many in the financial services industry, there remains an appetite for congressional action to codify standards and protections in this space. For example, the Financial Services Roundtable lauded the framework for its guidance and recognition of the threats faced by the nation's critical infrastructure, but said it would "continue to advocate for legislation to enhance, facilitate and protect cyber threat information sharing across the financial services industry, business sectors, law enforcement and the government."

Even as the Administration moves forward with its cybersecurity standards—reflecting a commitment by the President to seek ways in which to make progress even without legislation—there are a number of proposals in Congress that address cybersecurity and critical infrastructure. For example, Chairman Tom Carper (D-DE) of the Homeland Security and Government Affairs Committee (HSGAC) is planning to hold a hearing on the NIST framework now that it is finalized. While industry strongly believes the framework should be complemented by legislation that establishes liability protection for cyber threat countermeasures and information sharing, a number of factors have prevented proposed bills from moving forward. In addition to the privacy concerns that arise from information sharing proposals, cybersecurity legislation has been complicated by the debate over controversial NSA activities and a new congressional focus on high profile data breaches at nationwide retailers. Given these high profile data breaches, on which more can be found here, it could be possible for data breach legislation to be enacted independently as well as tied to a broader cybersecurity bill.

Another wrinkle in the process is the fact that several committees have jurisdiction over cyber issues making it unlikely a comprehensive bill will be developed. However, the House Homeland Security Subcommittee on Cybersecurity approved the National Cybersecurity and Critical Infrastructure Protection Act of 2013 (H.R. 3696) the first week of February, indicating some potential for cybersecurity legislation to move this year. On the Senate side, enacting cybersecurity legislation remains a priority for Chairman Jay Rockefeller (D-WV), so we may see a push for the Senate to act on the bipartisan Cybersecurity Act of 2013 (S. 1353), which was co-sponsored by Ranking Member Thune (R-SD) and approved late last year by the Commerce Committee, before Senator Rockefeller retires at the end of the year.

As Congress continues to debate the issue, financial industry regulators are beginning to take notice. The Securities and Exchange Commission (SEC) announced on February 14th that it would hold a roundtable in March to "discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns."