Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Delving Into FCC's 'Damn Important' Cybersecurity Report

Law360, New York (March 30, 2015, 3:41 PM ET) --

David S. Turetsky

On March 18, 2015, the Federal Communications Commission's industry-led advisory committee, the Communications Security Reliability and Interoperability Council, issued its final report on cybersecurity risk management, best practices and indicators of success. The report provides guidance and assistance tailored to each major sector of the communications industry for effective implementation of the Framework for Improving Critical Infrastructure Cybersecurity, a voluntary risk management tool developed in 2014 by the National Institute of Standards and Technology. Consistent with its charge by the FCC, the CSRIC also suggests voluntary mechanisms that industry can use to "give the Federal Communications Commission and the public assurance that communications providers are taking the necessary measures to manage cybersecurity risks across the enterprise."[1] This 415-page report is the most comprehensive effort to tailor and adapt the NIST Framework, which was designed to be useful across all critical infrastructure industries, for a specific industry. The report:

- identifies best practices and suggests specific priorities;

- provides a variety of tools and resources matched to communications providers of different sizes and types for voluntary use to manage cybersecurity risks;

- suggests mechanisms for communications providers to provide assurance that they are implementing sound risk management practices to reduce cybersecurity risks and identifies indicators of success; and

- recommends a path forward for policymakers and to help communications providers use and adapt the NIST Framework.

While the guidance in the report is vitally important for communications companies, it will also prove relevant for any company making use of the NIST Framework to help manage cybersecurity risks — even the companies that are not providers of critical infrastructure that have found the tool so valuable that they have voluntarily chosen to implement it. FCC Chairman Tom Wheeler, who had earlier challenged the private sector communications stakeholders to create a "new regulatory paradigm" of business-driven cybersecurity risk management, praised the effort that went into the report and called the work product "damn important."

Background

The NIST Framework was released in February 2014 and was developed pursuant to President Obama's Feb. 12, 2013, Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The executive order called for achievement of its goals, in part, through a public-private partnership that maintains "a cyberenvironment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties."

The NIST Framework is not a checklist or prescriptive mandate; rather it is designed to be a voluntary tool for individual companies to use to assess and manage cybersecurity risks in light of their unique needs, characteristics, threats, vulnerabilities, resources and risk tolerances.

The CSRIC is an FCC advisory committee led by industry that is composed of public, private and public-interest community participants. The Cybersecurity Risk Management and Best Practices was the final report produced by CSRIC's Working Group 4 and presented to the FCC. Working Group 4 was helmed by the commercial communications industry and included over 100 expert participants working in five major industry segments: broadcast, cable, satellite, wireless and wireline. The report suggests specific priorities and best practices for voluntary cybersecurity risk management in each of these segments and makes a variety of recommendations to companies, the FCC, NIST and others. The report is comprised in part of standalone reports from each of the industry segments and incorporates the work of five feeder groups: requirements and barriers to implementation; ecosystem shared responsibilities and collaboration; small and medium business; top cyberthreats and vectors; and measurement. Each of the feeder groups also included separate reports on their findings, which were informed in part by a dialogue with the various industry segments.

In sum, the project was designed to enhance cybersecurity not only by identifying assurances that could be provided voluntarily from industry to reflect that cybersecurity risks are actually being managed across an enterprise, but also by providing to industry best practices, use cases and sector-specific guidance to assist with voluntary implementation of the NIST Framework. The report also seeks, as does the NIST Framework, to provide information, and a common outlook and language for all relevant stakeholders inside and outside a communications company to understand these issues better and engage effectively, since cybersecurity is a matter for many disciplines, management, boards and others across industries.

Indicators, Assurances and Other Recommendations

The report identifies as a meaningful indicator of successful cyber-risk management the "availability of the critical [communications] infrastructure to deliver critical services." It embraces this benchmark as an "outcome-based measure."[2] In highlighting and explaining this choice, among other things, the report focuses on the role of critical infrastructure and the importance of network availability as a tool

for the public to seek help and obtain information in emergencies. The focus on "availability" also resonates with what many communications service providers are already obligated to report to the FCC under the Network Outage Reporting System (i.e., outages achieving a certain scale and impact).[3] The report notes that other types of measurements may require further work to be meaningful. These may include, for example, metrics that may make sense only if applied across sectors given the interdependencies among sectors, or could misleadingly suggest a worsening of cybersecurity when improved tools are able to detect more malware infections or hosted bots as compared to old tools.

In responding to the FCC's charge to recommend voluntary mechanisms to provide assurances that communications providers are taking the necessary steps to manage cybersecurity risks, the report suggests, among other things, three approaches:

1. that individual companies voluntarily hold confidential meetings to review their cybersecurity risk management processes, use of the NIST Framework or equivalent, and cyberthreats, cyberattacks and their responses with the FCC and U.S. Department of Homeland Security, which is the sector-specific agency already assigned certain relevant responsibilities for the communications sector;
2. that reporting on the effectiveness of communications sector cybersecurity risk management processes be included as a new part of the sector annual report that is produced in connection within a process for industry and governmental engagement at the DHS; and
3. that companies participate in a DHS voluntary program created in response to the executive order, sometimes called C3, that emphasizes converging critical infrastructure community resources to support cybersecurity risk management, connecting critical infrastructure stakeholders to the national resilience effort and coordinating critical infrastructure cross-sector efforts.

The report also includes a series of recommendations for the FCC, including leveraging a variety of resources and capabilities and promoting voluntary collaboration and facilitating threat information sharing, among other activities. It also concludes that cybersecurity information sharing is important and valuable, and reports that a barrier to it is Congress' failure so far to pass legislation that provides liability protection for companies that share.

Best Practices and Other Implementation Guidance

The report offers a wealth of information and assistance, and helpful use cases that illustrate applications of the NIST Framework. Importantly, it will help small businesses in each of the five industry segments to identify and prioritize specific risks and steps that can be taken to address them. It also identifies some of the most relevant threats and barriers to successful risk management. It is particularly helpful to small and medium-sized businesses seeking to implement the NIST Framework, breaking down more complex categories and analysis into questions of "what," "who" and "how" to simplify analysis and implementation. The NIST itself has recognized that more needs to be done for small businesses to implement appropriate risk management and recently sought public comment on the draft of a different and simplified cybersecurity framework for small businesses. Both the NIST and DHS have also stated that they are planning more outreach efforts to these types of companies.

The report includes practical analysis, noting the difficulty in determining risk exposure and the return on specific and general cybersecurity investments, including implementation of the NIST Framework. It highlights that cost is the single biggest barrier to implementing adequate cybersecurity, particularly for

smaller organizations. Moreover, the report notes that private companies of all sizes may be unable to withstand nation-state cybersecurity assaults and that big companies could be at risk from tens of thousands of connections to smaller players whose implementation of the NIST Framework to manage cybersecurity risk may not be determinable. It predicts a continued difficult attack environment and warns that "[i]t is not a matter of 'IF' a communications sector member will be attacked, but a matter of 'WHEN' they will be attacked, and that threat knowledge is essential to protect against attacks."[4]

While providing valuable assistance, the report is lengthy and complex, but that reflects the complexity of the topic, challenge and NIST Framework itself. The NIST Framework identifies five core functions: identify, protect, detect, respond and recover. Within those five functions it drills down via a total of 22 specific categories and 98 subcategories.

Next Steps

The FCC promptly issued a public notice on March 19 seeking public comment on the report's recommendations, including whether they or alternatives achieve the FCC's announced goals and other questions.

The communications industry is moving forward with various pilot programs. Industry also anticipates a meeting that includes the DHS and FCC and is expected to discuss next steps, particularly in connection with the voluntary assurances. In addition, there will be a series of outreach efforts organized to publicize, educate and engage industry concerning the report, the NIST Framework and related matters.

The CSRIC serves for two years and the report was issued on the final day of the term of this CSRIC (CSRIC IV). A new CSRIC (CSRIC V) is anticipated to hold its first meeting in June and will have some cybersecurity issues on its plate.

Conclusion

The report certainly is not a silver bullet — there are none when it comes to cybersecurity. It is the product, however, of an expert, intensive, industry-led effort with broad participation, and should be highly relevant and helpful to the communications services sector in managing cybersecurity risks. It has been well-received by industry, including associations such as U.S. Telecom, the CTIA - The Wireless Association, National Cable and Telecommunications Association and Telecommunications Industry Association, to name a few, favorably commented on by the FCC and NIST, and some state utility commissioners have expressed interest in following up on it. Communications companies of all sizes, with some help if needed, should review the report. They should evaluate and decide what in the report is helpful to them in their circumstances for making cybersecurity risk management decisions and what is not, and follow up accordingly. The report may also help to increase understanding of cybersecurity risk management in the communications industry by other industries that are interdependent, and help companies in almost any industry to gain some insights into how they might better apply the NIST Framework.

In fact, communications services providers ignore this tool at their own peril, notwithstanding that its use is voluntary and companies are not all in the same position and are not expected to make the same choices. First, as with any toolbox, doing without a tool that may be particularly well-suited to the task at hand can make it more difficult to succeed. For some companies, as a practical matter, it is possible that a failure to consider the substance of the report in some fashion could result in underperformance in making cybersecurity risk management decisions. If so, that could raise the risk of an outcome no

company wants.

In addition, given the nature and substance of the report and its warm embrace by industry and favorable response by regulators, it is possible that there could be legal and political risks to ignoring it, particularly in the event of certain types of breaches or outages.

—By David S. Turetsky, Michelle A. Reed and Greg W. Guice, Akin Gump Strauss Hauer & Feld LLP

David Turetsky is a partner in Akin Gump Strauss Hauer & Feld's Washington, D.C., office, where he oversees the firm's cybersecurity initiative. Prior to joining the firm, Turetsky was a senior official at the FCC, where he spent most of his tenure as chief of the FCC's Public Safety and Homeland Security Bureau.

Michelle Reed is a partner in Akin Gump Strauss Hauer & Feld's Dallas office.

Greg Guice is senior counsel in Akin Gump Strauss Hauer & Feld's Washington, D.C., office. Prior to joining the firm, Guice was the director of legislative affairs at the FCC and was counsel to the Subcommittee on Communications, Technology and the Internet for the House Energy and Commerce Committee.

[1] See page 4 of the report.

[2] See page 28 of the report.

[3] Part four rules.

[4] See page 26 of the report.