Cybersecurity Law Report
An Acuris company

cslawreport.com

March 9, 2022

CYBER CRIME

Securing Emerging Technologies Without Hampering Innovation: Private Sector Challenges

By Gregory R. Gonzalez, *Wilkinson Barker Knauer*

Emerging technologies have the prospect of enhancing our world in ways that we have yet to imagine. Several core technological advancements in areas such as 5G, quantum computing, and artificial intelligence/machine learning will allow people to interact with their surroundings in new ways, enhancing professional and personal opportunities, increasing our economic prosperity, and making our nation more secure.

In just a few years, it is possible that we will be liberated from certain daily obligations, allowing us to pursue those things that we value most. Autonomous vehicles could soon safely drive us on our daily commute and on family road trips. IoT devices may help us manage our homes more efficiently. Intelligent machines can make mundane work tasks a thing of the past.

We have already seen this progression unfolding. This is an amazing opportunity, but with it comes immense security challenges that threaten to disrupt our ability to use technology as it is intended – for the good of humanity.

This first article in a two-part series discusses innovation challenges, the need for more information sharing and government support, incident reporting issues and the Strengthening American Cybersecurity Act of 2022 that was unanimously passed by the Senate on March 1, 2022, and statistics on the private sector's investments in cybersecurity. Part two will cover government initiatives and what companies seeking to innovate can be doing now, including adapting the organization's cyber culture to today's risks.

See "The Intelligent Workplace in the Age of a Pandemic: Balancing Innovation and Risk" (Oct. 28, 2020).

Private Industry Bears Security and Regulatory Burdens

With every technological epoch there comes a concomitant increase in security risk, and the burden is borne by the numerous private sector industries that seek to advance these emerging technologies. Not only must they address the direct security risks to their innovations, but they also must operate in an increasingly challenging regulatory environment – one that has the capacity to inhibit their ability to dream up and implement the next generation of technologies.

For example, the highly regulated telecommunications industry provides the communications infrastructure that directly and indirectly facilitates all other technological innovation. Naturally, this industry faces some of the most complex security challenges of any. Malicious nation states want to exploit communications technologies for their military advantage to the detriment of the United States. These malicious nation states also seek to access the vast amounts of intellectual property, confidential business information and PII that transits our telecommunications infrastructure, seeking to capture a technical edge that will translate into economic advantage. Meanwhile, criminal syndicates flow through these systems surreptitiously seeking to exploit vulnerabilities that allow them to steal or ransom this valuable data for profit.

While remaining focused on a rapidly changing cyber-threat environment, organizations in the telecommunications sector are facing a barrage of Executive Orders, agency rulemakings and potential legislation, which could stunt innovation and growth.

See CSLR's two-part series on cybersecurity in a 5G world: "Vulnerabilities and Challenges" (May 12, 2021); and "Tackling the Challenges With Revised Strategies" (May 19, 2021).

Legislation and Regulation Can Inhibit Innovation

The federal government's focus and prioritization of cybersecurity and supply chain integrity is appropriate and commendable. However, it is seldom the case that broad, proscriptive legislation or regulatory measures provide optimal outcomes. Additionally, without being armed with accurate assessments of the adoption of the NIST Cybersecurity Framework 1.0/1.1, robust legislation and/or regulation would not be judicious, especially as we move towards Framework 2.0 (discussed in part two). All organizations, particularly those in the communications and other critical infrastructure sectors, are facing the prospect of a multi-layered statutory and regulatory regime that will increase cybersecurity compliance costs exponentially and risk inhibiting innovation over the long-term.

See "Senior Commerce Official Discusses Supply Chain Security and Cyber Policy" (Oct. 21, 2020).

Incident Reporting

Much of the focus of legislators and regulators has been on imposing cyber incident reporting requirements on the private sector. Most would agree that it is appropriate for the federal government to expect to receive timely information about cyber threats to critical infrastructure – in fact, critical infrastructure companies routinely share threat information with the government. DHS, the FBI and other federal entities need information from the private sector to fulfill their mission to disrupt these threats to national security.

While there are multiple incident reporting bills proposed in Congress, it was not clear whether any of these bills would pass both houses of the current Congress until the Russian invasion of Ukraine on February 24, 2022, which increased the prospect of cyberattacks on U.S. critical infrastructure. On March 1, 2022, the Senate unanimously passed S.3600, the Strengthening American Cybersecurity Act of 2022, which will require critical infrastructure organizations to report "covered cyber incidents" to DHS within 72 hours. The expectation is that the bill will be fast-tracked by the House and sent to the

President for signature forthwith. However, even if the bill were to be signed in the next few weeks, final rules are not required to be implemented for months after the legislation is signed. We would expect pressure to accomplish the rulemaking much sooner, but the rulemaking process is quite complicated, even for an apparently straightforward requirement such as this.

Prior to the passage of S.3600, agencies such as the FCC and SEC were seeking to invoke their regulatory power to achieve similar objectives, which would impact many communications sector organizations. It is not yet certain how the regulatory agencies are digesting and will react to the legislative developments, but the savings provision in Section 2242 of the bill appears to reflect the Senate's intention not to otherwise limit regulatory authority in the cybersecurity space through the new act.

Just a few months ago, the FCC Chairwoman circulated a concept for a Notice of Proposed Rulemaking that would have the FCC consider: (a) eliminating the current seven-business-day mandatory waiting period for notifying customers of a breach; (b) requiring carriers to notify the FCC, FBI and U.S. Secret Service of all "reportable breaches;" and (c) requiring notification of inadvertent breaches. If the seven-day waiting period were to be eliminated, it could require almost real-time notice to the government entities upon discovery of a "reportable breach," even inside of the 72-hour period provided for in S.3600. Such a requirement would have the potential to distract from a carrier's incident response, particularly if the definition of "reportable breach" were not aligned with the definition of a "covered cyber incident"; it would also have the potential to complicate any law enforcement investigation, should actionable evidence be disclosed to regulators contemporaneously.

Around the same time as the FCC Chairwoman made her announcement, the SEC Chair made clear that the SEC will also be considering whether to add more cyber event reporting requirements for public companies. Investors certainly have a right to make investment decisions based upon an assessment of a public company's approach to, and prioritization of, cybersecurity. However, any such terms that impose stringent public notice deadlines upon SEC-registered companies could further complicate incident response for companies that are already part of highly regulated critical infrastructure sectors.

See "Gensler Discusses the SEC's Cyber Priorities" (Feb. 2, 2022).

Government Contracts

Many critical infrastructure organizations also serve as government contractors and grant recipients. Executive Order (E.O.) 14028, issued by the President, in May 2021, requires government agencies to explore ways to amend standard contractual language to include provisions requiring the sharing of cyber threat and incident information with multiple agencies, including CISA and the FBI, based on a yet-to-be published scale of severity. Additionally, the E.O. directed NIST to develop criteria for an IoT security labeling program, as well as guidance to secure the software supply chain, including a Software Bill of Materials plan. Information and communications technology suppliers to the government continue to await final rules and contract terms that they will need to abide by, which may ultimately absorb significant compliance resources.

On the federal grant side, critical infrastructure organizations are expected to compete for billions of dollars, as part of the Infrastructure Investment and Jobs Act, signed into law in November 2021. Some portion of that will be administered by the Department of Commerce's National Telecommunications and Information Administration, which is also expected to impose cybersecurity protocols as part of its funding requirements.

See "CISA and DHS Counsel Explain Cybersecurity Executive Order's Key Provisions" (May 26, 2021).

Rapidly Increasing Private Sector Cybersecurity Investments

According to a report by Gartner, the global cybersecurity market was predicted to be $150 billion U.S. dollars in 2021. That number is projected to more than double to $346 billion by the year 2027, according to Astute Analytica.

A study from ABI Research predicts that cybersecurity spending in the telecommunications industry, and other critical infrastructure sectors, was to reach about $106 billion in 2021, increasing $9 billion year-on-year from 2020. The exponential growth trend in cybersecurity spending indicates that private sector organizations that develop and maintain critical infrastructure are taking their cybersecurity posture seriously, as are many other organizations.

Another sign of progress comes in the form of a report, from Momentum Cyber, that $29.3 billion in venture capital and private equity funding was invested in cybersecurity companies globally in 2021, up 136% over 2020.

While cybersecurity professionals understand that spending alone is not the way to address significant and growing security challenges, it is evident that market dynamics are fostering competition for the best technical solutions, which can be coupled with efforts to increase awareness within organizations about the cybersecurity threats they face daily, to create a holistic cybersecurity environment.

Need for Government Support

Private industry cannot create a holistic cybersecurity environment without support from the federal government. The emphasis from the government should be on unifying its policy approach, with primacy placed on the importance of information sharing.

Coordinated Efforts

It is a positive sign that the Executive Branch, Congress and independent Federal regulatory agencies are engaged on the issue of protecting the nation's valuable technological resources. However, the multiple lines of effort require private sector entities to devote significant resources to monitor the evolving policy landscape and identify opportunities to shape the outcomes without inhibiting growth. The U.S. government should prioritize and coordinate these efforts to enable private sector partners to devote more resources to developing the technologies that will ensure our future economic prosperity.

Information Sharing

The federal government clearly has a vital and prominent role in protecting the nation's economic ingenuity and the critical infrastructure that enables that ingenuity. Collectively, cyber threats pose a direct risk to our economic and physical security and, therefore, our national security. Corporations, particularly those producing and/or operating our critical infrastructure, such as those in the telecommunications sector, understand their obligation to the nation. They contribute to our security in many ways, including by sharing threat information with the government, lending technical experts to government-convened forums and helping to set baseline security standards. Some believe, however, that their contributions could be better reciprocated by the government.

It is much more difficult for the government to share classified or sensitive threat information with the private sector than it is to receive it. That is understandable. It appears, though, that the government may be considering ways in which it can be more nimble in declassifying information in a timely way so that it can be shared with the public when necessary. According to media reports, the Director of National Intelligence recently explained that "deficiencies in the current classification system undermine our national security, as well as critical democratic objectives, by impeding our ability to share information in a timely manner, be that sharing with our intelligence partners, our oversight bodies, or, *when appropriate*, *with the general public* [emphasis added]." This is not to suggest that in all, or even most, cases sharing of classified or otherwise highly sensitive information is warranted, but the government should consider expanding the ways that it can get specific, actionable and timely cyber intelligence to its private sector partners, for the collective good of the American people.

Gregory R. Gonzalez is a partner at Wilkinson Barker Knauer, LLP, in Washington, D.C. He is a former career Department of Justice national security prosecutor, intelligence lawyer and counsel to National Security Division leadership. Gonzalez served as a National Security Cyber Specialist for over seven years and received advanced cyber training as an inaugural National Security Division Cyber Fellow. In his final role with DOJ, he served as the Department's first Liaison to U.S. Cyber Command.