Cybersecurity Law Report
An Acuris company

cslawreport.com

March 16, 2022

TECH MEETS LEGAL

Securing Emerging Technologies Without Hampering Innovation: Government Initiatives and How Companies Can Adapt

By Gregory R. Gonzalez, *Wilkinson Barker Knauer LLP*

The relationship between the federal government and the private sector on matters relating to cybersecurity is evolving at an incredibly high pace. The landscape is being shaped daily as new successes and setbacks are brought to light.

The foundation for a positive outcome has been laid, but more can and should be done to solidify a workable relationship that enhances the private sector's capacity to innovate while the government protects critical and emerging technologies. Meanwhile, there are important steps that private sector organizations can take now, which will better prepare them to address cyber risks and will give confidence to policymakers that the collective national interest is being considered, even in the absence of compulsory rules.

This second installment of a two-part article series discusses government initiatives and what companies seeking to innovate can be doing now. Part one covered the challenges to innovation, and the need for more information sharing and government support.

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

One Successful Public-Private Engagement: NIST Cybersecurity Framework

The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework or Framework), first published by the Department of Commerce's National Institute of Standards and Technology, in 2014, is a very successful collaboration between government, the private sector and other civil society elements. At various points throughout the development process, stakeholders were able to contribute and help shape the outcome. The NIST Cybersecurity Framework is evolutionary, flexible and, most importantly, not proscriptive. Although initially targeted to critical infrastructure sectors, the Framework can guide organizations of all sizes, from all sectors, that are seeking to advance and mature their cybersecurity risk posture. It has been adopted by private sector organizations throughout the United States and internationally.

Recently, NIST published a Request for Information from private sector stakeholders, as it considers updating the Framework to version 2.0 to "account for the changing

landscape of cybersecurity risks, technologies, and resources." It appears that greater emphasis will be placed on supply-chain risk management in the next edition. This effort will foster positive engagements between the federal government and the private sector, giving the private sector an opportunity to shape the path forward and, ultimately, strengthening our collective security.

See CSLR's two-part series on NIST's new IOT standard: "Boosting Security As States Launch Laws" (Mar. 4, 2020); and "Inspiring a Wave of New Device Security Guidance" (Mar. 11, 2020).

Executive Branch Improvements May Lead to More Effective Private-Sector Partnership

According to a report, from December 2021, titled "Federal Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure," the Government Accountability Office (GAO) recommended that the federal government strengthen the federal role in protecting the cybersecurity of critical infrastructure. Understandably, most of this load falls on the Department of Homeland Security, and particularly the nascent Cybersecurity and Infrastructure Security Agency (CISA), which has an extremely challenging mission that it must fulfill as the organization matures.

One of the topline messages in the report was that private sector stakeholders from critical infrastructure sectors expressed concerns about challenges, including: (a) a lack of involvement in developing guidance, (b) a lack of timely responses, (c) inconsistent distribution of information, and (d) lack of access to actionable intelligence. Fortunately, according to the GAO, DHS accepted its recommendations for improvements and reported that it intends to fully implement the changes by the end of 2022.

In the December 2021 report, the GAO also reiterated its recommendation that agencies "better measure the adoption of the NIST framework of voluntary cyber standards and correct sector-specific weaknesses." The GAO noted that most sector risk management agencies were not collecting data about and reporting on improvements in the protection of critical infrastructure resulting from adoption of the Framework. According to the GAO, as of November 2021, none of the recommendations had been implemented, leaving government unable to accurately assesses the extent to which the 16 critical infrastructure sectors are better protecting themselves from cybersecurity risk. Hopefully, improvements in this area will coincide with the roll-out of NIST Framework 2.0, so that the federal government can accurately gauge the progress being made.

In November 2021, the GAO also issued a communications sector-specific report, noting that the "[c]ommunications [s]ector – comprised of broadcast, cable, satellite, wireless, and wireline systems and networks primarily owned and operated by the private sector – is an integral component of the U.S. economy and vital to national security. It underlies the operations of business, public safety organizations, and government." According to the report, the sector "faces serious…cyber-related… [and other] threats that could affect operations of local, regional, and national networks."

This report recommended that CISA, as the government agency responsible for the communications sector, assess the effectiveness

of its programs and services, so that it can "prioritize those efforts that are most useful or relevant to securing and strengthening resilience of [the sector] and the extent to which these activities are reducing risks." These conclusions suggest that improvements on the federal government side could result in increased effectiveness of its partnerships with the private sector, strengthening the nation's collective cybersecurity without adding any additional compliance burdens to our nation's innovators and those organizations which facilitate them.

Positive Collaborative Effort Underway

In the face of the uncertainty in the private sector, there is the prospect for meaningful expansion of the public-private partnership model between the private sector and the government. In August 2021, CISA launched a pilot program for the Joint Cyber Defense Collaborative (JCDC). Its mission is to "lead collaborative public and private sector cyber defense planning, cybersecurity information fusion and analysis, and the purposeful dissemination of cyber defense guidance to reduce cyber risks to our National Critical Functions." In addition to DHS, government partners include the Department of Justice, Department of Defense – including U.S. Cyber Command and the National Security Agency – and the Office of the Director of National Intelligence. These are the right government entities to bring to the table with critical infrastructure partners. The CISA Director said that the JCDC "will enable us to transform public-private partnerships into public-private joint action, and information sharing into information enabling – timely, relevant, and actionable."

This model may have already borne fruit. CISA announced, on February 28, that JCDC private industry member Broadcom, through the Symantec Threat Hunter Team, uncovered an advanced persistent threat (APT) campaign, attributed to Chinese threat-actors, against select governments and other critical infrastructure targets, including in the telecommunications, transportation, and manufacturing sectors. According to CISA, the Symantec team, with the assistance of PwC, worked with the agency, to identify victims of the malware ("Daxin") and assisted in detection and remediation. This tight public-private collaboration apparently provided CISA and its partners with an opportunity for quiet remediation of sensitive systems before a wider dissemination of threat information to the cybersecurity industry and public exposure of the threat actors.

The "Cyber Social Contract"

Calling for a "Cyber Social Contract," the National Cyber Director and a colleague recently wrote: "[t]he private sector must prioritize long-term investments in a digital ecosystem that equitably distributes the burden of cyber defense. Government, in turn, must provide more timely and comprehensive threat information while simultaneously treating industry as a vital partner. Finally, both the public and private sectors must commit to moving toward true collaboration — contributing resources, attention, expertise, and people toward institutions designed to prevent, counter, and recover from cyber incidents."

Creating and fostering the sense of shared risk, responsibility and cost is imperative to the collective goal of protecting and growing the ability to innovate in the face of rapidly

evolving cyber threats. If the government's momentum continues in the right direction, it will help foster innovation, allowing the U.S. economy to flourish and our national security to be maintained.

What Companies Should Be Doing Now

As the federal government's cybersecurity approach comes into focus, companies should remain proactive in their approach to cybersecurity: investing in worthwhile technologies and building a culture in which each employee views themselves as a cyber defender.

Adapt Organizational Culture to the Risk

The messaging about the importance of cybersecurity must come from C-suite leaders. There is indication that CEOs are increasingly emphasizing that messaging throughout their organizations. According to PwC's annual CEO survey for 2022, cyber risk came out as the top impediment to growth, exceeding health risks (which was top in 2021, unsurprisingly) and macroeconomic volatility. The cyber risk response was just a hair short of reaching a full majority (49%) for this year.

Importantly, of the CEOs who expressed that they were either "extremely concerned" or "very concerned" about cyber risks, 56% indicated that they believed such risks could inhibit their organization's ability to innovate through technology or process improvements. The corporate leaders who understand this risk to their organization's future are going to be willing to use all tools at their disposal – both technical and behavioral – to ensure that the organization's employees understand and address the risk from top to bottom.

Train

In one indication of the growing use of behavioral tools in the corporate environment, a cybersecurity workforce development company, Skillsoft, reported that it observed a 53% spike in the total number of annual hours employees spent on cybersecurity "upskilling" between 2019 and 2021. Training is especially important if pandemic-related adaptations to workforce distribution become permanent.

See CSLR's three-part guide to cybersecurity training: "Program Hallmarks and Whom to Train" (Oct. 16, 2019); "What to Cover and Implementation Strategies" (Oct. 23, 2019); and "Assessing Effectiveness and Avoiding Pitfalls" (Oct. 30, 2019).

Enlist Board Expertise

Another important step to enhancing an organization's security posture is to have cybersecurity expertise at the board level. A study from Gartner suggests that, by 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member. If this comes to fruition, it would be a fourfold increase over 2021 numbers.

See "Twelve Steps for Engaging the Board of Directors and Implementing a Long-Term Cybersecurity Plan" (Sep. 16, 2020).

Understand and Mitigate Threats

Increasingly, we have seen nation states with advanced capabilities using cyber as a vector to compromise intellectual property, confidential business files and PII. These nation-state hackers are highly skilled and have the resources (time and money), as well as a state-driven motive, to penetrate a

corporation's cybersecurity defenses – either directly or through a supply-chain attack – for economic advantage.

Private sector organizations need to supplement their technical cybersecurity investments by understanding the strategic motivations of malicious actors. These organizations also need to have a strong insider threat program to ensure that employees are not easily recruited into these schemes.

To complement their cybersecurity investments, those who are developing critical and emerging technologies should consider hiring experts who can guide them on the strategic dynamics shaping short-term and long-term geopolitical developments.

Further, companies should seek to understand the threats that they face that are unique to their organization. They should also consider the different avenues that are available to obtain information about the threats that they are facing, partnering directly with the FBI, DHS and other agencies that possess valuable threat intelligence, which may be shared bilaterally or as part of a broader, industry-focused engagement, enabling organizations to be even more proactive about their cybersecurity risk management. Every FBI field office in the country has a Private Sector Coordinator and cyber expertise.

See "Perspectives From the Public and Private Sectors on Information Sharing During COVID-19" (Jun. 24, 2020).

Engage in Corporate Initiatives

Major corporations also committed in August 2021 to initiatives to fill the cybersecurity workforce gap. While the federal government encouraged corporate leaders to take such steps, these are ultimately voluntary investments that will better prepare industries to address cyber risks – risks that only become more complex with the advent of new computing and telecommunications technologies.

See "Resilience CEO Explains Insurance Industry's Ambitious Initiative to Bolster the Nation's Cybersecurity" (Sep. 29, 2021).

Collaborate and Be Proactive

When other opportunities arise to demonstrate the company's commitment to cybersecurity to the federal government, such as a future invitation to join the JCDC, or another collaborative organization, leap in. This will help establish trust and provide further confidence to the government that the private sector is a reliable partner, even when the commitment is voluntary.

Also, when presented with the chance to shape the government's understanding of the issues and the best solutions, such as through public forums or rulemakings, take advantage of the ability to make your voice heard. The government is listening, and, in the end, it may result in a reduced compliance burden.

Gregory 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.