Cybersecurity Law Report cslawreport.com

Oct. 19, 2022

Incident Response

A New Era of Cyber Incident Reporting and Cybersecurity Regulation: How Companies Should Prepare and Engage

By
Gregory Gonzalez, Evelyn Remaley, Brian Murray, Clete Johnson, Savannah Schaefer, Morgan Schick and Karina Bohorquez,
Wilkinson Barker Knauer LLP

A new era of cybersecurity policy in the United States launched in March 2022 – just weeks after Russia's invasion of Ukraine, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), giving the Cybersecurity and Infrastructure Security Agency (CISA), within the Department of Homeland Security, its first, and perhaps not last, rulemaking authority. CIRCIA creates legal protections and provides guidance to companies that operate in critical infrastructure sectors, including a requirement to report cyber incidents within 72 hours, and report ransom payments within 24 hours.

This second installment of a two-part article series identifies areas of particular concern to the most significant critical infrastructure sectors, including financial services, communications and energy, and discusses the future of cybersecurity regulation in the United States. Part one examined important provisions of CIRCIA that CISA, with industry input, will shape through the rulemaking process.

See "Lessons From CISA for In-House Counsel on Mitigating and Managing MSP Breach Threats" (Jun. 29, 2022).

Potential Impact of CIRCIA on Critical Infrastructure Sectors

Companies in the financial services, energy and communications sectors have disparate cybersecurity incident reporting obligations to various federal, and in some cases state, regulators. All publicly traded companies in those sectors are now facing the prospect of having to also contend with SEC incident reporting requirements. Below, we identify some of the challenges companies in these

sectors currently face, which we believe should be considered by CISA and the CIRC before adopting new rules for CIRCIA.

Financial Services Sector

Industry Make-Up

According to the Financial Services Sector Specific Plan (last issued in 2015), the sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities. The sector is highly diverse, and each financial institution has unique security and resilience needs.

Relevant Regulators

Gramm-Leach-Bliley and Dodd-Frank provide federal regulators with significant authority to impact the cybersecurity governance practices of entities in the financial sector. The Federal Reserve Board, Commodity Futures Trading Commission (CFTC), FTC, and SEC have all instituted policies that require sector participants to meet certain standards intended to ensure the continued operation of markets and the protection of sensitive financial data, which include, in some circumstances, limited incident reporting requirements.

Interplay With SEC Reporting Rules

Currently, the SEC's proposed cyber incident reporting rules, published shortly before the enactment of CIRCIA, are pending and, if adopted, would subsume a much broader group of publicly traded financial services companies and investment advisers and funds. According to the SEC in the Notice of Proposed Rulemaking (NPRM), it would not "expect a registrant to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." Nonetheless, the amendments to Form 8-K would require a registrant to publicly disclose details about the incident, including:

1. when it was discovered and whether it is ongoing;
2. a brief description of the nature and scope of the incident;
3. whether any data was stolen, altered, accessed or used for any other unauthorized purpose;
4. the effect of the incident on the registrant's operations; and
5. whether the registrant has remediated or is currently remediating the incident.

The CIRCIA confidentiality provisions do not just benefit covered entities, they allow for operational coordination between CISA and its federal partners, including law enforcement and intelligence

agencies. However broad and generalized, data points from an 8-K about an SEC-covered cybersecurity incident could be exploited by sophisticated nation-state and criminal hackers to determine whether the victim has a complete understanding of the scope of the intrusion and whether it might be all-clear to activate any resident persistent access tools. No investigative advantages, to companies or law enforcement partners, should be yielded in the immediate aftermath of an incident, even though the interest of investor transparency is legitimate and understandable. Although the SEC explained in the NPRM that it had considered law enforcement and cyber-defensive interests and determined that "[o]n balance, it is our current view that the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay," we believe that the SEC will face significant pressure from the CIRC to at least abandon its insistence on a four-business day filing requirement.

Even if the SEC pulls back, banking organizations covered by the 2021 banking regulators' incident reporting rule will still need to comply with the existing requirement to report to their primary federal regulator, within 36 hours, incidents that have materially disrupted or degraded, or are reasonably likely to materially disrupt or degrade, a banking organization's ability to carry out banking operations. Further, CFTC-regulated entities (including swap execution facilities, designated contract markets and swap data repositories) must "promptly" report qualifying cybersecurity incidents and "targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity." The CIRC's anticipated concern about the SEC-proposed rule will not likely extend to these other sector rules to the same degree, however, because there is no public disclosure component that could potentially compromise an active investigation while incident response is ongoing.

See Cybersecurity Law Report's two-part series on SEC cyber rules: "How to Prepare for the New 8-K Incident Mandate" (Aug. 10, 2022); and "How to Prepare for the New 10-K Disclosure Mandates" (Aug. 17, 2022).

NYDFS Requirements

CIRCIA also does not preempt state cyber incident reporting requirements. Currently, the New York Department of Financial Services (NYDFS) Part 500 Cybersecurity Requirements for Financial Services Companies requires covered entities to notify the superintendent of certain cybersecurity events as promptly as possible, but no later than 72 hours from a determination that a reportable event has occurred. That requirement is triggered whenever the covered entity is required to provide notice to any government body, meaning that NYDFS-covered entities will need to file a report to NYDFS whenever a CIRCIA report is filed with DHS. In pre-proposed revisions to Part 500, published in July 2022 (but now absent from the NYDFS website), NYDFS indicated its intent to add a 24-hour ransomware payment reporting requirement. This is an indication that NYDFS may be seeking to align its cybersecurity reporting rules with CIRCIA, although, in the ransomware context, the revised New York rules would further require "justification" for payment of a ransom and evidence of sanctions due diligence.

See "Cybersecurity Compliance Lessons From NYDFS' Carnival Action" (Aug. 3, 2022).

Energy Sector

A Vulnerable Industry

As detailed in the Energy Sector Specific Plan (last issued in 2015), the sector is composed of three interrelated subsectors – oil, electricity and natural gas. The sector is vast and faces a tremendous variety of threats, which each organization assesses differently. The sector's vulnerabilities are particularly concerning to national security officials, given its enabling function across all other critical infrastructure sectors – providing essential fuel and electricity that powers communications networks and financial institutions.

The DOE, DHS, Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC) (a not-for-profit international regulatory authority responsible for the continental United States, Canada and the northern portion of Baja California, Mexico) all exercise respective authorities to regulate and provide guidance on cybersecurity standards in the energy sector.

See "Infrastructure Cybersecurity Challenges: A View Through the Oil and Gas Pipeline Lens" (May 3, 2017).

Electricity Providers

FERC has federal oversight over NERC, which is responsible for assuring efficient and effective risk reduction to the security and reliability of the electrical grid. The Energy Policy Act of 2005 authorized FERC to set cybersecurity standards for the Bulk Electric System (BES). As such, NERC developed the Critical Infrastructure Protection (CIP) Reliability Standards, which includes cybersecurity reporting requirements for the BES. Any owner or operator of BES in the United States must be CIP compliant. In 2018, FERC directed NERC to broaden CIP by expanding the definition of a "reportable cyber security incident" to include "incidents that might facilitate subsequent efforts to harm the reliable operation of the BES." NERC then developed a revised version of the cyber incident reporting standard, in effect as of this writing, that requires reporting within one hour of a reportable cyber security incident and by the end of the next calendar day after a determination that a reportable cyber security incident was an attempt to compromise certain high and medium impact operational technology systems.

Pipeline Operators

Like electricity providers, pipeline operators also must comply with cybersecurity incident reporting requirements. Under emergency authority granted by the Aviation and Transportation Security Act of 2001, the Transportation Security Administration (TSA) issued two emergency directives, in the wake of the 2021 Colonial Pipeline attack, requiring cyber incident reporting and imposing cyberattack mitigation measures. The original prescriptive directives expired in 2022 and, in their place, TSA issued a more flexible directive, perhaps recognizing the drawbacks of the prior approach. Pursuant to the new directive, owners and operators of TSA-identified "critical" intrastate and interstate pipeline operations and infrastructure must report cybersecurity incidents to CISA no later than 24 hours after the incident is identified, which extended the 12-hour reporting timeline imposed by the original directive.

See "How Colonial Pipeline Changed Advice on Ransomware Preparation and Response" (Apr. 6, 2022).

Utilities

Utility commissions from every state and U.S. territory are authorized to impose cybersecurity requirements on entities such as public power utilities or electric cooperatives. In fact, many state public utility commissions have already issued such cyber incident reporting requirements. Yet, if an entity is also part of the BES, it remains subject to FERC regulations. Presumably, many of these state-regulated entities will also be covered under CIRCIA's incident reporting requirements. Given the lack of a preemption provision in CIRCIA, and the CIRC's inability to prohibit conflicting federal regulations, it is very possible that energy companies will have to contend with multiple cybersecurity incident reporting requirement regimes indefinitely.

Communications Sector

Five Segments

The communications sector includes diverse entities subject to a range of existing reporting requirements. The Communications Sector Coordinating Council distinguishes between five segments of network owners and operators – broadcast, cable, satellite, wireless and wireline – and includes an array of communications network suppliers that often support connectivity across many of the 16 critical infrastructure sectors designated under PPD-21.

Network Outage Reporting

Network providers already comply with numerous reporting requirements. Through the Network Outage Reporting System, communications providers must report to the FCC information about significant disruptions that could affect homeland security, public health or safety and the economic well-being of the nation. Wireless providers, for example, must:

1. notify the FCC within two hours of discovering a reportable outage, whether caused by a cyber event or otherwise;
2. submit an initial report to the FCC within three days; and
3. submit a final report with more detailed information within 30 days.

Data Breach Reporting

Network providers are also subject to special data breach reporting requirements under the FCC's rules for Customer Proprietary Network Information (CPNI). Upon reasonable determination of a CPNI breach, a telecommunications carrier must: notify law enforcement as soon as practicable, but no later than seven business days after determining the breach occurred; and notify customers of or publicly disclose the breach no sooner than seven days after notifying law enforcement, unless state laws direct otherwise, a carrier believes there is an extraordinarily urgent need to notify certain customers, or the investigating agency determines disclosure would compromise the investigation or national security. Earlier in 2022, the FCC Chairwoman announced that she circulated a proposal to her fellow commissioners to update these rules. She proposed eliminating the seven-day customer notification waiting period and expanding the notification requirements to cover "inadvertent breaches," among other things.

Potential Conflicts

As CISA considers the application of CIRCIA requirements to the communications sector, it will need to understand how its 72-hour reporting requirement will operate in cases where a covered cybersecurity incident results in a network outage or CPNI data breach. Additionally, if the SEC adopts its proposed requirement for public companies to disclose within four business days of a material cyber incident, some telecommunications companies and the law enforcement agencies working with them to respond to cyber incidents could find themselves at odds with conflicting reporting and disclosure timelines.

Many network providers will also be subject to new cybersecurity requirements under infrastructure funding programs. For example, the National Telecommunications and Information Administration (NTIA) will require companies providing network infrastructure and services to state broadband funding recipients to attest that they have a cybersecurity and supply chain risk management plan in place that aligns to certain federal guidelines. These plans must align with guidance from the National Institute of Standards and Technology (NIST)'s Cybersecurity Framework (CSF), the standards and controls in E.O. 14028, and various NIST guidance documents on supply chain risk management. States must submit these plans to NTIA upon request. The FCC is considering whether to require similar attestations from beneficiaries of its own funding programs and from providers who distribute emergency alerts. It is very possible that such requirements will flow down throughout the communications technology supply chain through contractual agreements with communications companies receiving this funding.

Future of Cybersecurity Regulation in the United States: The European Model?

While CISA's attempt to formulate a cyber incident reporting scheme for critical infrastructure is just getting underway, legislative developments could result in a more exacting regulatory treatment for entities deemed "systemically important" critical infrastructure. Companies subsumed into this category could be required to meet certain "performance goals" and be subject to examinations akin to those currently required of "operators of essential services" (OESs) in the European Union, as part of the Network and Information Systems Directive (NIS Directive), the first piece of E.U.-wide legislation addressing cybersecurity, which was enacted in 2016 and implemented by Member States in 2018.

Some entities in the financial services, energy and communications sectors, and in other critical infrastructure sectors in Europe, fall under the NIS Directive. The NIS Directive requires Member States to identify OESs for enhanced cybersecurity regulation, including baseline security requirements and incident notification when there is a "significant impact" on operational continuity. The NIS Directive also provides regulators with the authority to issue binding instructions to OESs to prevent and/or remedy cybersecurity incidents.

E.U. leaders found that implementation of the NIS Directive across Europe was challenging, resulting in fragmentation across Member States. In response, a provisional agreement on the text of "NIS2" was reached between the Council of the E.U. and the European Parliament on May 13, 2022. Once

adopted (likely to occur before the end of 2022), NIS2 will replace the NIS Directive and Member States will have 18 months to transpose NIS2 into national law. Instead of relying on the discretion of Member States, NIS2 will be self-executing for entities meeting the "essential entities" criteria (if they have more than 250 employees and either have a greater than €50-million annual turnover or a €43-million balance sheet). NIS2 will also impose a hard incident reporting deadline of 24 hours for an initial incident report, whereas the NIS Directive only required that a report be filed "without undue delay." NIS2 will also allow for pre-incident checks, scans and audits, and will direct Member States to ensure their authorities have *ex post* supervisory power over important entities.

At the same time, the E.U. is seeking to implement the Digital Operations Resilience Act (DORA) as a financial sector-specific regulation, which, if approved, will apply to a broader set of sector participants. DORA will establish governance rules; baseline risk management; system requirements; third-party risk assessments and standards; testing and verification; information-sharing; exercises and inspections; and incident reporting requirements. Both NIS2 and DORA include significant financial penalties for non-compliance.

Next Steps

Although it took an armed conflict for the United States to enact cybersecurity incident reporting legislation for critical infrastructure, the cybersecurity paradigm has shifted permanently. In addition to CIRCIA, U.S. government departments and agencies are preparing to invoke their authority in ways that reflect a potential desire to tilt towards active, prescriptive regulation. For instance, the FCC launched an inquiry, earlier in 2022, into cybersecurity risks to the Border Gateway Protocol (BGP), which is central to the internet's global connectivity. While the security risk from BGP re-routing is well-documented and the government's efforts to mitigate that threat are entirely legitimate, the FCC's authority to impose BGP security measures is questionable. The inquiry has, however, been officially supported by CISA, as well as jointly by the Departments of Justice and Defense, all of which encouraged the FCC to consider regulation to address gaps in voluntary approaches to this issue.

Such data points and statements should be examined closely by private industry for signs that the U.S. government is moving away from its commitment to the collaborative, partnership-based approach to U.S. cybersecurity. In response, companies should consistently remind the government of the progress that has been achieved using the cooperative model and point out the risks inherent in a compliance-based model, leveraging both the formal procedural vehicles that are now being established to facilitate industry input and the more informal interactions and relationships that companies already have with relevant regulators.

See "How to Prepare for the Cybersecurity Incident Reporting for Critical Infrastructure Act" (Aug. 3, 2022).

Gregory Gonzalez is a partner at Wilkinson Barker Knauer (WBK), 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 was designated as a National Security Cyber Specialist for over seven years and received advanced cyber training as a National Security Division Cyber Fellow. In that role, he successfully investigated and prosecuted a first-of-its-kind national security-cyber

case. In his final position with DOJ, he served as the Department's first Liaison to U.S. Cyber Command. At WBK, Gonzalez counsels clients on a wide array of national security, cybersecurity and data privacy matters.

Evelyn Remaley is a partner at WBK. Before joining the firm, she was Acting Assistant Secretary of Commerce for Communications and Information, and Acting Administrator of the National Telecommunications and Information Administration, an Executive Branch agency, part of the Department of Commerce, that is principally responsible for advising the President on telecommunications and information policy issues. In that role, Remaley was also responsible for leading the Department's cybersecurity policy efforts. Prior to her federal service, she led a cybersecurity and internet policy team at Booz Allen Hamilton, where she oversaw efforts supporting a wide range of cyber policy and governance projects for the Departments of Defense and Homeland Security.

Brian Murray is a partner at WBK. He has been a practitioner of communication law in private practice for two decades. Murray's substantive experience encompasses cybersecurity, the regulatory treatment of IP-based services and the implications of foreign investments in the U.S. He is also well-versed in many traditional telecommunications and media regulatory issues.

Clete Johnson is a partner at WBK and a U.S. Army veteran. Prior to joining WBK, he served as a senior cybersecurity counsel in a variety of roles in the national security and intelligence communities, including as Professional Staff for the Senate Select Committee on Intelligence, Chief Counsel for Cybersecurity at the Federal Communications Commission, and Senior Adviser for Cybersecurity and Technology to the Secretary of Commerce, serving as the Commerce Department's primary staff representative for National Security Council deliberations on cybersecurity matters.

Savannah Schaefer is an associate at WBK. Prior to joining WBK, she led cybersecurity policy development for two technology and telecommunications-focused trade associations. She served in leadership roles on the Information Technology Sector Coordinating Council and the Department of Homeland Security's ICT Supply Chain Risk Management Task Force, and as a member of the Communications Sector Coordinating Council. Additionally, Schaefer served as a fellow at the Federal Communications Commission.

Morgan Schick is an associate at WBK. She advises clients on a wide array of communications issues, including network security, public safety and wireless resiliency.

Karina Bohorquez is an associate at WBK. Prior to joining WBK, she interned with Freedom Technologies Inc., NTIA's Office of Policy Analysis and Development, T-Mobile government affairs, and USTelecom's policy and advocacy team.