Reprinted with permission of Law360

Preparing For New Mandatory Cyber Reporting Rules

By **Steven Stransky and Lacy Rex** (March 25, 2022)

Steven Stransky

Lacy Rex

On March 15, President Joe Biden signed into law a federal spending bill containing the Cybersecurity Incident Reporting for Critical Infrastructure Act, which mandates that certain private sector entities notify the Cybersecurity and Infrastructure Security Agency when they suffer a cyber incident or make a ransomware payment.[1]

Although the Cybersecurity Incident Reporting for Critical Infrastructure Act, or CIRCIA, reporting requirements will not become operational until CISA publishes its implementing regulations, which could take several months, businesses should begin assessing whether their incident response plans account for some of the law's key provisions.

Organizations also need to closely monitor cyber reporting regulations set forth by other federal agencies as they may be amended in the near future to more closely align with CIRCIA and avoid imposing duplicative reporting obligations on the private sector.

CIRCIA: Reporting Timeframes, Liability Protections and Enforcement

The federal government has implemented several cybersecurity-related programs and policies to encourage broader cyberthreat information sharing among, and between, the private sector and federal, state, and local governments.

However, many organizations choose not to voluntarily participate in these programs, which consequently prevents the government from gaining access to important data and metrics related to malicious cyber actors.

Accordingly, Congress passed CIRCIA with the expectation that mandatory cyber reporting will increase greater cyberthreat information sharing with federal agencies, which will assist in generating timely intelligence on constantly evolving cyberattack tactics, trends and procedures.

CIRCIA does not apply to all private sector organizations, but, rather, only to a subset of critical infrastructure organizations designated by CISA as covered entities.

As background, there are 16 critical infrastructure sectors: chemical, communications, dams, emergency services, financial services, government facilities, information technology, nuclear facilities, energy, critical manufacturing, food and agriculture, health care, commercial facilities, transportation systems, water and wastewater systems, and defense industrial base organizations.

Each covered entity will be required to report to CISA within 72 hours after the entity reasonably believes that a covered cyber incident occurred. Essentially, a covered cyber incident is malicious activity that jeopardizes the confidentiality, integrity or availability of a covered entity's information system, or the data retained or transmitted thereon.

These entities are also required to promptly submit supplemental cyber reports if they

discover substantially new or different information related to the incident.

Separately, if a covered entity is subjected to ransomware, or a similar cyberattack, and submits a ransomware payment in exchange for regaining access to its information systems or data, CIRCIA mandates that such a covered entity must report this payment to CISA within 24 hours.

CISA is responsible for issuing regulations that implement several aspects of CIRCIA, including the format and mechanism by which cyber incident and ransomware payment reports can be submitted and the specific content each report must contain.

CIRCIA contains several liability protections for organizations that comply with the law's reporting requirements. For instance, it provides that no legal claims can be maintained in any court arising from the submission of a cyber incident or ransom payment report.

It also prohibits — with some limited exceptions — a federal, state or local authority from using information solely derived from a covered cyber incident or ransom payment report to undertake a regulatory or other enforcement action against the covered entity.

Notwithstanding these general liability protections, CIRCIA sets forth important enforcement authorities. For instance, CISA is granted the authority to issue subpoenas to covered entities to enforce compliance with the law and compel the disclosure of information related to cyber incidents and ransom payments. The failure to comply with a subpoena can result in an organization being held in contempt of court.

CIRCIA Compliance and Incident Response Plans

An incident response plan is a predetermined set of policies and procedures intended to detect, respond to and mitigate the damages arising from a malicious cyberattack. Although CISA is responsible for issuing future regulations to implement CIRCIA, there are several areas of compliance that businesses should understand and incorporate into their incident response plans.

Security Controls

CIRCIA was enacted against the heightened risk that businesses might be targeted or otherwise impacted by a malicious cyber actor as part of the Russia-Ukraine war.[2] In fact, the White House stated that "Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs" imposed on Moscow by the U.S. and its allies.[3]

Accordingly, organizations should ensure that their incident response plans, and their corresponding information security programs, align with industry recognized data security frameworks, such as the National Institute of Standards and Technology's cybersecurity framework.

Recently, the U.S. government identified several of the most important technical, physical and administrative security measures that organizations should implement to mitigate risk in this area, — e.g., multifactor authentication, antivirus and anti-malware scanning, encryption and network traffic filtering — and this guidance could serve as key resources for businesses when assessing their incident response plans.[4]

Training employees on proper cyber hygiene practices, such as regular password changes,

is strongly recommended for building a solidified first line of defense.

Incident Response Team

Given the narrow timeframes in which a covered entity needs to report a cyber incident and ransomware payments to CISA, it is important that an organization quickly assemble an incident response team composed of the stakeholders who will have responsibilities in responding to the incident.

More specifically, the incident response plan should identify and provide contact information for all primary and secondary incident response team members, including for internal employees, external IT consultants, outside counsel, ransomware negotiators, insurance brokers and insurance carriers. It's important to review the incident response vendors with an insurance broker in advance of a cyber incident to ensure they are approved on the carrier's panel.

This issue may be complicated when essential personnel and contractors are located in multiple cities and countries, and incident response plans should take into account geographical diversity when identifying incident response team members.

In addition, the incident response team must include individuals or organizations that can undertake the appropriate diligence to ensure ransom payments are not furnished to groups listed on a sanctions list or otherwise affect export control laws.[4] Of course, organizations should also coordinate with their insurance carrier prior to making any such ransomware payment to better understand their ability to recover losses.

Communication Plans

In response to a cybersecurity event, including a ransomware attack, organizations need to have a clear and concise communications strategy to ensure they are providing timely and relevant information to regulatory authorities and others affected by the incident, e.g., employees, customers and investors.

Importantly, CIRCIA expressly allows third parties, such as law firms, insurance carriers and IT consultants, to submit cyber incident and ransom payment reports to CISA on behalf of the covered entity. Accordingly, an organization should identify in its incident response plan, and prior to an incident, whether it will authorize a third party to facilitate CISA reporting and clearly define all applicable roles and responsibilities in this area.

Evidence Preservation

Evidence preservation is a key part of an incident response plan because organizations need to ensure that their response efforts do not compromise key information related to a cyber incident, such as audit logs, files or similar records that may be needed in the event of litigation or to file an insurance claim.

Such evidence preservation is also important for the purpose of CIRCIA compliance as the law mandates that the covered entities preserve evidence related to their reporting obligations, although the scope of this issue is to be set forth by CISA in future regulations.

In turn, an incident response plan should define how an organization will, in the event of a cyber incident or ransomware attack, secure access to its IT systems, networks and devices to maintain their integrity; retain access logs; execute chain of custody documentation; and

issue litigation holds.

Legal and Evidentiary Privileges

As organizations respond to cyberattacks, they need to consider potential legal risks to their business, such as a civil action resulting from a compromise to personal information during the cyber event. Accordingly, organizations commonly ensure that information and data discovered in their incident response efforts are subject to legal and evidentiary privileges and protected from discovery in the event of litigation.[6]

Importantly, CIRCIA provides that when a covered entity submits a cyber incident or ransom payment report to CISA, such reporting shall not constitute a waiver of any applicable privilege or protection provided by law, which presumably extends to the attorney-client privilege and work product doctrine.

Accordingly, organizations should ensure that their incident response plan includes their outside counsel as a part of their incident response team and certify that their counsel is preapproved by a cyberinsurance carrier.

Duplicative Reporting and More Regulations

One of the primary concerns with introducing the new federal cyber reporting law is that organizations could be subject to multiple cyber reporting obligations and have to exert time and resources to comply with these disparate frameworks.

To remedy this concern, CIRCIA envisions a process whereby CISA will execute an agreement with other federal agencies that have issued their own cyber reporting regulations to ensure CISA has readily available access to such information.

This is significant because covered entities that are legally or contractually required to report cyber incidents and ransomware payments to a federal agency, other than CISA, are exempt from submitting similar reports to CISA.

This exception is intended to avoid duplicative reporting. But it is only available to covered entities if CISA actually executes these types of information sharing arrangements with other federal agencies, and if the underlying reporting obligations to the other federal agency have similar reporting timeframes and content requirements as set forth in CIRCIA.

Given the broad range of existing and pending cyber reporting obligations, it will be important to see how federal agencies amend their own regulations to align with CIRCIA, if at all, in order to minimize reporting obligations on the private sector.

For example, existing data breach notification regulations governing protected health information allow victims of a cyberattack to report such incidents within 60 days, or in accordance with an annual reporting framework, depending on the scope of the incident. This is well beyond CIRCIA's 72-hour reporting obligation.

Accordingly, covered entities should diligently monitor regulatory activity to identify whether their existing cybersecurity reporting obligations are amended to more closely mirror CIRCIA and ensure they comply with any new framework.

Steven G. Stransky is a partner and co-chair of the privacy and cybersecurity practice group at Thompson Hine LLP. He is also an adjunct law professor at the Frederick K. Cox International Law Center at Case Western Reserve University School of Law. He formerly served as a deputy legal adviser on the president's National Security Council.

Lacy Rex is a vice president at Oswald Companies.

[1] Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, H.R. 2471, 117th Cong., 990-1011 (2022).

[2] Steven G. Stransky, et. al., Anticipating Cyberinsurance Wartime Exclusion Questions, Law360 (March 8, 2022); John Dermody, Counsel, O'Melveny & Myers LLP, Interview with Fox News (Feb. 23, 2022).

[3] The White House, Statement by President Biden on our Nation's Cybersecurity (March 21, 2022).

[4] The White House, Fact Sheet: Act Now to Protect Against Potential Cyberattacks (March 21, 2022); The Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation, Joint Bulletin, AA22-057A, "Destructive Malware Targeting Organizations in Ukraine" (March 1, 2022).

[5] Steven G. Stransky, et. al., "Treasury Department Issues Updated Advisory on Ransomware Payments," Thompson Hine LLP, International Trade Update (Sept. 23, 2021).

[6] Steven G. Stransky and Kemba Walden, "Cyber Reporting Proposals: Assessing Liability Protections and Legal Privileges," Lawfare Blog (Feb. 17, 2022).