4 Considerations In Light Of Cyber Incident Notification Bill

By **Colin Jennings, Ericka Johnson and Genevieve Bresnahan** (August 9, 2021)

Colin Jennings

Ericka Johnson

Genevieve Bresnahan

In light of recent, high-profile ransomware attacks against critical U.S. infrastructure, lawmakers have been grappling with the most appropriate course of action to combat ransomware attacks.

Ransomware is a type of malicious software that is designed to prevent legitimate owners and operators of an information system from accessing their information technology environment. This allows threat actors to extort payments, i.e., ransom, in exchange for a decryption key allowing the organization to regain access to its systems or data.

More recently, threat actors have also stolen organizations data and threatened to publish sensitive documents if the organizations refuse to pay. Unfortunately, it is generally more cost-effective for an organization to pay a ransom, usually through a digital currency, than to restore the data itself.

Likewise, payments in exchange for the promise to destroy stolen data generally lower the risk of litigation and/or regulatory enforcement for the ransomware victim. With the increasing prevalence of cyberinsurance, threat actors continue to demand higher ransoms, knowing that an insurance carrier with deep pockets will bear the cost.

For these reasons, ransomware attacks have become more focused, sophisticated, costly and increasingly targeted at critical U.S. infrastructure, i.e., those industries like energy or healthcare with deep pockets and a dire need to regain operability. Given the national security implications, lawmakers appear to be at an inflection point, unified around the understanding that something needs to be done, though the mechanics and scope of any legislative action have been nebulous at best.

This recently changed when members of Congress took the first significant step to doing just that. On July 21, Sen. Mark Warner, D-Va., Chair of the Senate Intelligence Committee, along with Vice Chair, Sen. Marco Rubio, R-Fla., and Sen. Susan Collins, R-Maine, introduced the Cyber Incident Notification Act.

The bipartisan legislation would require, at a minimum, federal agencies and contractors, and owners and operators of critical infrastructure to report potential cybersecurity intrusions to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency no later than 24 hours after the confirmation of such an intrusion. However, the act leaves many of the details on the implementation of this legislation up to regulators.

For example, the act leaves it to the secretary of the DHS and others to define when a notification obligation is triggered and what information organizations will have to share when making notification of the threat to the federal government. While lawmakers also leave it to the DHS secretary, and others, to define cybersecurity intrusions, the definition must include ransomware, signaling lawmakers' intent to combat the proliferation of

ransomware attacks.

Likewise, while lawmakers further leave it to the secretary and others to define critical infrastructure and, therefore, the applicability of the mandatory reporting provision to private companies, this pending legislation will likely apply to companies that operate in the healthcare, transportation, financial services, agriculture, energy and information technology sectors because incapacity or destruction would leave a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.

Implementing a federal law requiring these organizations to disclose details of a cyberattack — e.g., threat actor group, ransom date, demand, extortion fee, cryptocurrency wallet, transaction hashes, etc. — may assist law enforcement in understanding the scope and scale of the crime, track the societal impacts of cyberattacks, and enable better targeting of disruptive activities.

However, there is some concern among the private sector that mandatory reporting could put organizations in further legal trouble should notice result in further regulatory investigation and/or action.

Further, another mandatory notification obligation may place an undue burden on companies already encumbered by having to meet data breach notification laws in 54 American states and territories, federal reporting requirements for certain industry sectors, and notification obligations around the world.

No matter the debate, lawmakers agree that something needs to be done to mitigate the national security threats posed by cybersecurity attacks. Accordingly, organizations should consider the following in assessing their preparedness to meet the demands of this pending and future legislation.

1. Regulatory enforcement of critical infrastructure will be robust.

Following the lead of the Biden administration, regulatory enforcement of companies that operate in the healthcare, transportation, financial services, agriculture, energy and information technology sectors will likely be robust.

In an executive order on improving the nation's cybersecurity, implemented following the ransomware attack on Colonial Pipeline Co., which left thousands on the East Coast under a temporary gas shortage, President Joe Biden stated that, "[i]t is the policy of my Administration that the prevention, detection, assessment and remediation of cyber incidents is a top priority and essential to national and economic security."

While the executive order signals the administration's support of increased regulatory oversight of existing cybersecurity laws in the interest of national security, the act further signals bipartisan support for increased oversight of critical infrastructure organizations.

Accordingly, we can anticipate that regulators will set requirements above and beyond those outlined in the legislation and will more thoroughly review an organization's preparation for and response to a cyberattack — particularly an attack that publicly affects the American people. Should a regulator discover that such organizations failed to comply with existing cybersecurity laws and regulations, we can anticipate swift and public regulatory action.

2. Regulators will likely be on notice of cyberattacks against critical infrastructure.

There is some concern among the private sector that mandatory reporting could put organizations in further legal trouble, should the report be publicly available and/or could form the basis of a regulatory or other enforcement action. Fortunately, the act mitigates this concern by providing that the notice cannot be admitted into evidence in a civil or criminal action, except for an action for failure to comply with the act, nor can the notice be subject to the Freedom of Information Act.

Notwithstanding that, nothing in the act prevents regulators from conferring with CISA, or otherwise, regarding the existence of a cyberattack and/or the content of the notice. Accordingly, given the mandatory notification requirement, regulators will likely be on notice. Further, the act requires organizations to preserve data related to the cyberattack, though the exact nature and scope of the preservation requirement is left to the DHS secretary and others to define.

Accordingly, nothing in the act prohibits regulators from requesting/subpoenaing such records and further investigating the incident. Whereas organizations could once fly under the radar with no disclosure obligation, those days are gone, and organizations should be prepared for more diligent regulatory investigations.

3. A plan is necessary to meet the notification obligation in a timely manner.

No later than 24 hours after the potential cybersecurity intrusion, the act requires critical infrastructure organizations to notify DHS. For perspective, as a practical matter, this requires organizations to identify a cyber incident within its IT environment, discern that the threat meets the act's definition of a cybersecurity intrusion, identify and potentially retain the appropriate experts to make the notification to DHS, and draft and file the appropriate notice.

Without a detailed plan in place, organizations are putting themselves in a precarious position to miss this deadline — especially since failure to comply with the act could result in a civil penalty of up to 0.5% of private organization's gross revenue from the prior year for each day organizations continue to fail to report.

Further, regulators generally will request a copy of a company's incident response plan as evidence of a company's due diligence, or lack thereof, in preparation to identify vulnerabilities and mitigate the risk of a cyberattack and its impact on the American people. Failure to produce a robust incident response plan will raise immediate red flags with regulators and may lead to further investigations.

Finally, the notification obligation also applies to nongovernmental organizations that provide cybersecurity incident response services. As such, should an organization decide against notification, its retained cybersecurity incident response firm would still be obligated to do so.

Accordingly, as a practical matter, this is an opportunity for organizations to review their existing incident response plan and ensure, among other things, they have a plan in place to make appropriate notifications to regulators in as soon as 24 hours, if necessary.

4. Organizations need to implement reasonable security measures.

Given this rapidly changing landscape, it is essential that critical infrastructure companies implement reasonable security measures, in anticipation of potential cyberattacks and increased regulatory scrutiny.

The act mandates that organizations include in their notifications descriptions of the "vulnerabilities leveraged" by the cyberattackers, as well as actions taken to mitigate the intrusion. For that reason, regulators will be on notice of a company's due diligence, or lack thereof, prior to a cyber incident.

Accordingly, companies should prioritize identifying and mitigating it cybersecurity risks. To do so, organizations should consider conducting a security threat risk assessments under privilege to identify potential vulnerabilities, while protecting the risk assessment itself from discovery during litigation.

Next, organizations should endeavor to remediate any known vulnerabilities and invest in security software and employee training, as appropriate. In doing so, companies can demonstrate to regulators that the organization exercised diligence in working to mitigate the risks of a potential cyberattack.

While there may not yet be a consensus on the appropriate course to mitigate the risk of cyberattacks, lawmakers appear to agree that something needs to happen, and the act is not only the first significant legislative text outlining what that action might look like, but it has strong bipartisan support. Accordingly, whatever course of action they take, private companies must be prepared for increased involvement from and potential reporting to the federal government.

Colin R. Jennings is a partner, Ericka A. Johnson is a senior associate and Genevieve L. Bresnahan is an associate at Squire Patton Boggs LLP.