What Private Cos. Can Learn From Biden Cybersecurity Order

By **Colin Jennings and Ericka Johnson**

Colin Jennings

Ericka Johnson

Americans were recently riveted by scenes of panic buying at the pump after a ransomware attack shut down the Colonial Pipeline Co., a critical source of fuel for the entire East Coast. For the first time, many reflected on the national security implications of cybersecurity attacks on everyday life — and the U.S. government swiftly responded. On May 12, President Joe Biden signed an executive order on improving the nation's cybersecurity.

The order aims to make significant contributions to modernizing the federal government's cybersecurity practices under an aggressive timeline. Broadly, the order directs several federal agencies and the heads of each federal civilian executive branch agency to share information, strengthen cybersecurity practices and deploy technologies that increase resilience against cyberattacks.

For the private sector, the order signals that the administration will likely support increased regulatory oversight of existing cybersecurity laws and regulations, as well as new cyber-related legislation. In the order, Biden provides that it is the policy of his administration "that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security."

Accordingly, regulators of existing cybersecurity laws and regulations — e.g., state offices of attorneys general, the Financial Crimes Enforcement Network, the Office of Foreign Assets Control, the Office of Civil Rights, etc. — are on notice of the administration's priorities.

Likewise, we are already seeing bipartisan movement to address cybersecurity issues beyond the reaches of Biden's order. Sens. Mark Warner, D-Va., and Marco Rubio, R-Fla., respectively the chairman and vice chairman of the U.S. Senate Intelligence Committee, are working to draft legislation that would require mandatory reporting of cyber incidents.

Warner has also indicated that he is working with officials in the Biden administration as well as Sens. Gary Peters, D-Mich., and Rob Portman, R-Ohio, the chairman and ranking member of the Senate Homeland Security and Governmental Affairs Committee, on advancing cybersecurity legislation that would affect the private sector.

Given the anticipated increase in regulatory oversight and legislative developments, Biden's order provides the private sector with a useful blueprint for modernizing their own cybersecurity practices. Indeed, the order was meant to be as such. The president notes in the order that "[t]he private sector must adapt to the continuously changing threat environment … [and the] Federal Government must lead by example."

While the order generally applies to the federal government and certain federal contractors, it provides the private sector with a guide for modernization of their own cybersecurity practices in anticipation of increased regulatory oversight and new legislation.

Identify and Protect Sensitive Data

Threat actors commonly steal sensitive data — i.e., personally identifiable information or business confidential information — and extort payments from victim organizations in exchange for the promise to delete the stolen data.

Threat actors prey on organizations' fears that the stolen data may be used to commit fraud against the very individuals or organizations whose data the organization was trusted to protect. Accordingly, organizations often pay a ransom to mitigate the risk of harm to such individuals or organizations, as well as to reduce the risk of reputational harm and litigation.

Recognizing this common tactic, the order requires the heads of federal civilian executive branch agencies, in consultation with several other federal agencies, within 90 days to evaluate the types and sensitivity of their respective agency's unclassified data and provide a report based upon such evaluation.

The report must prioritize unclassified data considered to be the most sensitive and under the greatest threat, and provide a detailed plan for appropriate processing and storage. To the later point, the order directs that within 180 days all federal civilian executive branch agencies adopt multifactor authentication and encryption of data, at rest and in transit, to the maximum extent possible.

Accordingly, the order provides some best practices for the private sector. Organizations should, likewise, consider periodically conducting a thorough data-mapping exercise to identify and memorialize the types and sensitivity of their respective data.

During the course of data-mapping exercises, organizations often discover data that no longer has a legitimate business purposes. By appropriately disposing of unneeded sensitive data, organizations can mitigate their risk of an extortion event. Further, in the event of a cyber incident, organizations can quickly understand which data may have been compromised and more efficiently meet any associated legal obligations.

Develop an Incident Response Plan

At the onset of a cyber incident, an organization's immediate action or inaction has a direct impact on the effectiveness of the overall response. In particular, within the first 72 hours, an organization generally needs to contain the incident, expel the threat actor if applicable, preserve forensic evidence for later analysis and determine any immediate legal obligations. Accordingly, having a well-rehearsed and coordinated plan to respond is vital to an effective response.

Recognizing the government's existing deficiency, the Biden's order notes that currently cybersecurity vulnerability and incident
response procedures, used to identify, remediate and recover from vulnerabilities and incidents, vary greatly across agencies, hindering a comprehensive and effective government response.

Accordingly, the order directs federal agencies to develop within 120 days a standard set of procedures — a playbook — to be used in the planning and conducting of cybersecurity vulnerability and incident response activities.

For the private sector, cyber incidents are no longer a matter of if, but of when. Following this best practice from the order, organizations should consider creating their own incident

response plans.

A plan generally identifies members of an incident response team, comprised of key personnel within the organization, e.g., information technology, human resources, in-house counsel, communications, etc., as well as outside experts, e.g., outside counsel and their retained IT forensic team. Immediately upon detection of a cyber incident, this team may be recalled to assist.

A plan also implements, among other things, disaster recovery procedures in the event that communications or automatic operations are no longer viable, and sets forth procedures for communicating with employees, business partners and/or employees.

Finally, to be most effective, a plan should be well-rehearsed so that the organization can quickly and efficiently respond.

Conduct Due Diligence on Third Parties

Most organizations in the private sector share some form of sensitive information with their third-party business partners. For example, organizations may share their financial information to make payments, or share proprietary or trade secret information to develop or manufacture a product or service. Given the proliferation of cyber incidents, third-party breaches are now another source of risk for organizations.

The executive order recognizes this dynamic. In particular, the order recognizes that the federal government contracts with information technology and operational technology service providers who process and host government data.

Given that these contractors are susceptible to cyber incidents, the order directs certain federal agencies within 60 days to propose recommended contract language and requirements to be put into the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.

The revisions generally aim to ensure that these federal contractors collect and preserve data relevant to cybersecurity event prevention, detection, response and investigation, as well as report cyber incidents and participate in investigations.

Likewise, given that the federal government purchases software, the order notes that the government must take action to rapidly improve security and protect the integrity of the software supply chain. The order directs that within 30 days certain federal agencies, with inputs from the government, the private sector and academia, develop guidelines to enhance the security of the software supply chain. As part of this initiative, the order contemplates a pilot program for a cybersecurity consumer-labeling program, to inform consumers about the security of software products.

The private sector can take a cue from these requirements. First, organizations should consider conducting due diligence on third parties to ensure that they have reasonable IT security measures in place to mitigate the risk of a cyber incident. Organizations, particularly those providing proprietary or trade secret information, should not be shy about inquiring into the particular IT controls in place — e.g., encryption, multifactor authentication, etc. By doing so, organizations can understand and mitigate the risk that their information may be compromised by third parties.

Next, while negotiating third-party contracts, organizations should ensure that the contract

includes a notification-obligation provision in the event of an unauthorized disclosure of business confidential information within a certain time period. This will allow organizations to take efficiently the steps necessary to mitigate the misuse of their data.

Implement IT Controls

Cyber criminals are becoming increasingly sophisticated, leveraging ever evolving software, tactics and tools to compromise government and industry IT environments. For that reason, it is imperative that organizations consider proactively implementing IT controls to identify active threats, harden their IT environments to withstand cyberattacks, and preserve evidence for analyzing the nature and scope of the inevitable cyber incident.

Recognizing the need to keep pace with today's dynamic and increasingly sophisticated cyberthreat environment, the order aims to achieve these requirements across the enterprise of the federal government.

In particular, to increase the federal government's ability to see threats, the order requires federal civilian executive branch agencies to deploy endpoint protection and response initiatives, to support proactive detection of cybersecurity incidents. Likewise, the order directs that within 90 days certain federal agencies are to provide a report on how current authorities are being utilized to engage in threat-hunting activities to seek out threat actors and thwart their efforts.

Likewise, to harden IT environments, the order directs agencies to prioritize the adoption and use of cloud technologies to store data. To preserve evidence, the order also directs the creation of policies for logging, log retention and log management, which will ensure centralized access and the accessibility of critical data for analysis in the event of a cyber incident.

While proactive IT controls in the private sector should be tailored to the needs of individual organizations, the order provides a good blueprint of the types of security controls that should be considered. These include access controls, endpoint protection, email security, network security, logging, monitoring and threat hunting.

In the event of a cyber incident, regulators and litigants generally inquire into an organization's due diligence to mitigate the risk of a cyber incident. In proactively implementing IT controls, organizations can mitigate their risk of an attack as well as the follow-on repercussions of a regulatory enforcement action or civil litigation.

Remediate Following a Cyber Incident

Finally, following the completion of a cyber incident, organizations are best positioned to reflect on any lessons learned, memorialize best practices that were effective during the response, and identify and remediate any critical vulnerabilities that lead to the cyber incident in the first place.

The executive order recognized the importance of such. The executive order directs the establishment of a Cyber Safety Review Board, to review and assess, with respect to significant cyber incidents affecting the federal and nonfederal systems, threat activities, vulnerabilities, mitigation activities, and agency responses. The board will be convened by the secretary of the Department of Homeland Security and be comprised of representatives from several federal agencies and representatives from private sector cybersecurity or software suppliers.

Following the Biden order's lead, the private sector should contemplate using this opportunity to conduct some formal review to identify critical vulnerabilities in its IT controls and organizational response and remediate the same, as necessary.

To do so, an organization should conduct a security threat risk assessment that provides clear recommendations for improvement. Following the recommendations of an assessment will mitigate the risk of a future attack and allow an organization to represent that it has conducted its due diligence in responding.

Cybersecurity is no longer an issue that exists on the periphery. The Biden administration's officials will continue prioritizing cybersecurity and their respective enforcement of cybersecurity laws and regulations, to protect the everyday American and the country's economic recovery more broadly.

Congress is likely to continue negotiating new legislation in committee and send a bill to the president's desk. For businesses of all sizes, industries and locations, this means conducting due diligence to mitigate the risk of cyberattack, and being prepared to respond when they occur.

Colin Jennings is a partner and Ericka Johnson is a senior associate at Squire Patton Boggs LLP.

Matthew Wagner, an associate at the firm, contributed to this article.