Ransomware: Fulfilling New Federal Compliance Obligations and Assessing Preparedness to Thwart or Respond to Attacks

By Shawn A. Morgan[1] and Joseph Carpini, Steptoe & Johnson PLLC

A. Colonial Pipeline Ransomware Attack

The Colonial Pipeline is the largest fuel pipeline system in the United States. The Georgia-based company, Colonial Pipeline Company transports about 45% of all fuel consumed on the East Coast, shipping gasoline, diesel fuel, jet fuel, and other refined petroleum products from the Gulf Coast of Texas 5,500 miles to northern New Jersey. On May 7, 2021, Colonial Pipeline suffered a massive ransomware attack. Ransomware attacks encrypt computer systems and seek to extract payments from the system operators in exchange for a key to regain access to the sensitive data. DarkSide, a hacker group believed to have roots in Eastern Europe, is thought to be the culprit.

On the morning of May 7, 2021, a Colonial Pipeline employee found a ransom note from the hackers on a control-room computer. The company's CEO, Joseph Blount, later confirmed that the company elected to make a $4.4 million ransom payment and explained that executives were uncertain of how badly the company's systems had been breached and how long restoring operations would take. Due to the immense potential impact of an extended shutdown of the transport of so much fuel to the East Coast, the company prioritized restoring operations as soon as possible; however, despite Colonial Pipeline's payment of the ransom, the decryption tool provided by the hackers proved insufficient to immediately restore operations, and the pipeline was shut down for six days.

Although the federal government is not often involved in the response to private sector cyber-attacks, in light of the widespread impact of the attack on Colonial Pipeline, the Cybersecurity and Infrastructure Security Agency (CISA) quickly sought information from Colonial Pipeline about the attack to attempt to learn how it occurred and how to ensure hackers could not repeat a similar attack in the future. Colonial Pipeline elected to share information with CISA, as well as the FBI and the U.S. Department of Energy; however, in the weeks since the attack, other federal agencies are also mandating information sharing under certain circumstances. Businesses must therefore be mindful of how these new compliance obligations may impact their work.

B. United States' Response

1. Executive Order 14028 - Largely in response to the Colonial Pipeline attack, as well as the recent cyber-attacks on SolarWinds and Microsoft Exchange, President Biden issued Executive Order 14028 on May 12, 2021, with the broad goal of improving cybersecurity defenses. The Executive Order calls for updated contract language for IT service providers contracting with the federal government to remove contractual barriers preventing service providers from sharing

[1] *Shawn A. Morgan (shawn.morgan@steptoe-johnson.com) leads the Cybersecurity Team at Steptoe & Johnson PLLC.*

information with the government. The Order also requires such service providers to share breach information that could impact government networks.

By updating the federal government's cybersecurity standards and establishing baseline security standards for the development of software sold to the government, the Biden administration hopes for a trickle-down effect that will improve private sector security standards and to enhance businesses' security performance. The Executive Order creates a "standardized playbook" for cyber incident response by federal departments and agencies, increases efforts to detect malicious cyber activity on federal networks, and establishes a Cybersecurity Safety Review Board. The Cybersecurity Safety Review Board is to be co-chaired by government and private sector leads and may convene to analyze significant cyber incidents and recommend steps to prevent repeat incidents, similar to the way the National Transportation Safety Board issues reports after airplane crashes. Federal legislation also has been introduced in a further effort to prevent future ransomware attacks on the country's energy infrastructure.

2. FERC - Even before the Executive Order was finalized, the Federal Energy Regulatory Commission (FERC) issued a statement on May 10, 2021, urging renewed action to secure and safeguard the nation's energy infrastructure. Chairman Richard Glick noted that although FERC "has established and enforced mandatory cybersecurity standards for the bulk electric system" for over 10 years, "there are no comparable mandatory standards for the nearly 3 million miles of natural gas, oil, and hazardous liquid pipelines that traverse the United States." He further explained:

> It is time to establish mandatory pipeline cybersecurity standards similar to those applicable to the electricity sector. Simply encouraging pipelines to voluntarily adopt best practices is an inadequate response to the ever-increasing number and sophistication of malevolent cyber actors. Mandatory pipeline security standards are necessary to protect the infrastructure on which we all depend.

3. TSA - FERC Chairman's comments appear to have also spurred the Transportation Security Administration (TSA) to enact new mandates for critical pipeline and natural gas facility owners and operators. The directive indicates that TSA determines whether a pipeline or facility is "critical" based upon a number of factors, including volume of product transported, service to other critical sectors, etc., referring to section 1557(b) of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. 110-53 (121 Stat. 266; Aug. 3, 2007) (9/11 Act) (codified at 6 U.S.C. § 1207).

On May 28, 2021, the TSA issued a directive, effective until May 28, 2022 requiring critical pipeline and natural gas facility owners and operators to take three steps to strengthen cybersecurity. First, cybersecurity incidents must be reported to CISA within 12 hours of the incident being identified. Second, owners and operators must designate a Cybersecurity Coordinator who is required to be available to TSA and CISA at all times to coordinate cybersecurity practices and address any incidents that arise. Finally, natural gas facility owners and operators are required to review their current activities and TSA's pipeline cybersecurity

recommendations to assess cyber risks, identify gaps in activities, develop remediation measures, and then report the assessment results to TSA and CISA.

4. DOJ - On June 3, 2021, the United States Department of Justice (DOJ) sent internal guidance to the U.S. Attorney's Offices across the country, requiring investigators to begin sharing details of their investigations with other federal authorities. DOJ will also seek to elevate investigations regarding ransomware attacks to the same priority currently given to terrorism-related matters.

C. Important Considerations for the Private Sector

1. Compliance Obligations Related to Information Sharing - As the federal government's focus on proactively combatting ransomware attacks sharpens, businesses must vigilantly monitor the evolving directives, regulations, and policies. TSA's edict in particular imposes significant reporting obligations on critical pipeline and natural gas facility owners and operators. Likewise, Executive Order 14028 places similar responsibilities on IT service providers contracting with the federal government. Understanding these requirements–or seeking advice of counsel if it is unclear whether the directives apply – is key to ensuring compliance with the law. Compliance, in turn, improves preparedness.

2. Preparedness - Because ransomware attacks are a threat to all companies, large or small, in addition to following applicable information sharing rules, businesses can take discrete steps to prepare for the unfortunate possibility of a cyberattack.

First, businesses should create planned responses in the event targeted by ransomware. Conducting a tabletop exercise, in which essential staff gather to discuss a simulated attack, is a good way to create a plan and assess preparedness. Discussions regarding a simulated attack may include topics including the following:

- availability of backups to restore damaged computer networks,
- the time and expertise needed to install the backups and restart operations,
- whether the company is willing to pay a ransom instead to regain access to its systems,
- the maximum ransom it may be willing to pay,
- who is qualified to "negotiate" the ransom, and
- how to handle media inquiries and customer/investor communications.

Involving counsel and board representatives in a tabletop exercise also aids in getting the most robust plan in place.

Additionally, businesses should assess the extent to which they can and are willing to share ransomware attack information with the government, beyond what may be required by law. In the past, companies are reticent to share their private information; however, as cyber-attacks become more sophisticated and inflict more economic and reputational damage, businesses may be motivated to readily share information to mitigate the consequences of a cyberattack or reduce the likelihood of an attack.

Finally, when anticipating the possibility of a paralyzing ransomware incident, businesses should evaluate the sufficiency of their resources to remediate a breach. Considering the sheer size of the Colonial Pipeline system and the scope of the attack it suffered, the speed with which Colonial was able to restore operations suggests that it had effectively prepared for a potential attack and that it had significant resources in place to respond to the attack. To assess available resources that may be needed to respond to a ransomware attack, businesses should consider:

- insurance coverages and limits,
- technical safeguards on computer networks and systems,
- third-party vendor security issues,
- the advance engagement of a cybersecurity vendor to help restore systems to full operations as quickly as possible, and
- what training employees might need now to minimize the possibility of falling prey to phishing schemes that can introduce ransomware.

Counsel can provide pre-incident guidance and review insurance policies and third-party vendor agreements. And, in the event of an attack, a business should contact outside counsel immediately for assistance in investigating and remediating the situation. Although cyber-attacks pose a real and significant risk, a company can best protect itself through advance planning, preparedness, and by engaging with experienced counsel.