11-Council on Foreign Relations

The Colonial Pipeline Incident Shows the Need for Broader Thinking about Cyber Resilience *[Disappointment]*

While there has been a great deal of recent debate about the respective roles of offense and defense in cybersecurity, the Colonial Pipeline episode highlights that a core policy challenge remains cultivating the resilience of U.S. critical infrastructure.

Blog Post by Guest Blogger for Net Politics

Erica D. Borghard is a senior fellow in the Technology and International Affairs program at the Carnegie Endowment for International Peace. Shawn W. Lonergan is a senior director in the cyber, risk, & regulatory practice at PricewaterhouseCoopers.

Colonial Pipeline, which operates one of the largest pipelines in the United States, chose to shut down thousands of miles of pipeline as a result of a ransomware cyberattack that the Federal Bureau of Investigation attributed to the Russian criminal group, DarkSide. This incident came on the heels of the Institute for Security and Technology's release of a task force report on combating ransomware. Cybersecurity experts have been sounding the alarm about the threat posed by ransomware *[Worry]* and, specifically, its use by criminal organizations for years. In 2019, there were over 100 known ransomware attacks perpetrated against state and local governments, including large American cities like Baltimore and Atlanta. And more recently, the Microsoft Exchange hack, linked to China, raised the possibility of criminal actors exploiting network vulnerabilities to conduct ransomware attacks.

While there has been a great deal of recent debate about the respective roles of offense and defense in cybersecurity, the Colonial Pipeline episode highlights that a core policy challenge remains cultivating the resilience of U.S. critical infrastructure. At an organizational level, cyber resilience

involves anticipating and preparing for adverse cyber events (whether they stem from nation-state or criminal entities); *[Disappointment]* withstanding and rapidly restoring critical systems and processes when cyber incidents inevitably occur; and learning as an organization in their wake.

Policymakers have been paying more attention to cyber resilience. The U.S. Cyberspace Solarium Commission's March 2020 report, for example, contains a range of policy measures aimed at this. The Biden administration tapped Caitlin Durkovich, who has a cybersecurity background, to serve as senior director of resilience and response on the National Security Council. On the private sector side, resilience has long been a prominent concern as industry grapples with how to invest in it and develop and promulgate standards and best practices.

However, what is publicly known about the Colonial Pipeline incident illustrates an important gap in current thinking about resilience *[Disappointment]*. Much of the conversation around cyber resilience focuses on how organizations can rapidly restore services and resume operations following disruptive or destructive cyber events. For the most mature organizations, these types of resilience measures include backup strategies, data vaulting, implementing zero-trust architecture, and cloud migration.

The ability to rapidly restore services and reduce the impact of disruptions is foundational to any cyber resilience program. While it is not yet clear whether it was Colonial Pipeline's proactive measures that mitigated the consequences *[Neutral]* of the cyberattack, or its decision to pay the nearly $5 million ransom, the company was able to restore service within a matter of days. *[Positive]* But these types of resilience measures are only part of the answer. One of DarkSide's and other criminal groups' tactics, techniques, and procedures (TTPs) is that if an affected entity refuses to pay the demanded ransom—perhaps because that organization has measures in place to recover lost data—then the group will threaten to publicly expose exfiltrated sensitive information (also known as "doxing"). On the Dark Web, DarkSide has posted stolen data from affected entities that refused to pay ransom, potentially causing reputational harm, liability exposure, or

loss in share value if an organization is publicly traded. In other words, quickly restoring services—itself a significant feat—could be insufficient.

Organizations could apply a range of measures to mitigate the consequences of doxing. For example, organizations could implement data loss prevention measures to more rapidly alert network defenders to anomalous behavior and prevent the exfiltration of sensitive information. For example, in the case of Colonial Pipeline, DarkSide was able to abscond with over 100 gigabytes of data in two hours. This activity should trigger defensive controls *[Disappointment]* and further investigation. While this will not prevent all exfiltration, these measures could limit its scale and create additional opportunities for detection if the threat actor is not fully aware of the triggers that could set off an alert to defenders. In other words, even though threat actors will inevitably adjust their TTPs, more robust data loss preventing controls will force a slower and more methodical exfiltration from the threat actor, increasing the potential period of detection.

From a policy-making perspective, a big challenge with ransomware is that companies have an incentive to keep information about incidents surrounding ransomware activity private—particularly if they decide to pay the demanded ransom *[Disappointment]*. This limits the ability of the government or other potentially affected entities (or the private cybersecurity providers they hire), which could be targeted by the same threat actor or by other threat actors employing similar tactics, from having a more complete understanding of the threat environment. This perspective is important to be able to adapt investments in controls and defensive postures to keep pace with the changing threat environment. Keeping incidents private has other negative implications for the broader ecosystem —it diminishes information available to insurers and others to model risk and accurately price products; it undermines the education of political leaders and the public at large; and so on.

Improving reporting requirements could help to address this gap. Some reporting requirements already exist, particularly for regulated industries and publicly traded companies; and other elements of energy sector are more closely regulated. However, many requirements do not sufficiently incorporate up-to-date cybersecurity best practices and are not necessarily

consistent across different stakeholders. Therefore, policy actions like updating requirements in the Sarbanes-Oxley Act to more systematically take into account cybersecurity; institutionalizing Security and Exchange Commission guidance on cybersecurity risks; and passing a National Data Breach Notification Law (all of which were recommended by the Cyberspace Solarium Commission) would lead to notable improvements. The Biden administration's recent executive order is a step in the right direction, particularly with respect to breach notification requirements, but it only directly affects federal government information systems and acquisitions (although it could have broader positive spillover effects). To influence the broader private sector ecosystem, given that regulators are an important drivers of industry behavior, regulatory requirements should be more adaptable to changing environments.

Although DarkSide apologized for the geopolitical consequences of its ransomware attack and announced that it was disbanding, other criminal groups could not be as circumspect about targeting critical infrastructure in the future. Resilience standards should not become simply a compliance checklist and the goals of resilience are not simply recovery and the continuity of operations. Rather, there needs to be a more agile understanding of what it means to be resilient as an organization in an evolving threat environment.