Armstrong Teasdale

May 17, 2021 • Advisory • www.atllp.com

THE LEGAL IMPACT OF THE COLONIAL PIPELINE RANSOMWARE INCIDENT

Last week, ransomware gained so much attention that even cybercriminals appeared caught off guard. As reported by Krebs on Security, after a $5 million ransom payment was obtained from Colonial Pipeline, the administrator of a Russian cybercrime forum stated "[t]here's too much publicity" with ransomware and that it has "become dangerous and toxic."

Setting aside the questionable consciences of cybercriminals, the Colonial Pipeline incident more than other recent high-profile cybersecurity incidents – e.g., SolarWinds, Microsoft and Accellion – is likely to expand legal obligations relating to cybersecurity because of notable events that occurred before, during and after the incident.

AN ENFORCER AGAINST RANSOMWARE EMERGES

On March 31, 2021, Department of Homeland Security (DHS) Secretary Alejandro Mayorkas outlined a roadmap for DHS' cybersecurity strategy. Referring to a series of 60-day "sprints" to begin implementing the strategy, he stated that DHS' first focus is on raising ransomware awareness and disrupting those who launch the attacks.

DHS has designated the Cybersecurity & Infrastructure Security Agency (CISA) as its cybersecurity quarterback. On its website, CISA has a substantial library of ransomware resources including ransomware prevention best practices and a response checklist. These resources have evolved just as the types of ransomware variants have evolved and provide important information that should be considered when developing and refining cybersecurity incident response plans.

A TASK FORCE PROPOSES A RANSOMWARE RESPONSE FRAMEWORK

On April 29, 2021, a team of more than 60 experts from software companies, cybersecurity vendors, government agencies, nonprofits and academic institutions released an 81-page report titled "Combating Ransomware."

The goal of the task force, similar to DHS and CISA's, is "to proactively and relentlessly disrupt the ransomware business model through a series of coordinated actions." In its report, the task force published 48 actions divided into four categories, the last two relating to how organizations prepare for and

PEOPLE

Jeffrey Schultz, CIPP/US

F. Scott Galt, CIPP/E

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

respond to ransomware attacks.

The task force noted that in 2020, nearly 2,400 organizations were victims of ransomware and that they:

- averaged 21 days of downtime;
- averaged 287 days to fully recover;
- altogether paid $350 million in ransoms; and
- averaged $312,493 per payment.

The task force then recommended the following:

- Being Prepared
    - A framework should be developed to provide organizations with a ransomware-specific risk assessment tool.
    - Awareness materials should be developed to assist organizational leaders about the needs and risks of ransomware.
    - Regulatory guidance on how organizations can reduce the likelihood of fines or other penalties should be provided with preparation recommendations.
    - Incentivizing alignment with an established risk management framework should be encouraged, including tax breaks for meeting certain baseline standards.
- Knowing How to Respond
    - Rapid information sharing should occur between organizations that are affected by a ransomware incident.
    - A standardized incident reporting format and network should be created.
    - Organizations should be required to conduct a cost-benefit assessment prior to making a ransom payment.

THE WHITE HOUSE DEMANDS BETTER CYBERSECURITY

On May 12, 2021, President Biden issued the “Executive Order on Improving the Nation’s Cybersecurity.” The 18-page order includes numerous ambitious requirements with deadlines ranging from 14-360 days and is divided into sections relating to, among other things:

- removal of contractual barriers to information sharing;
- mandated use of multifactor authentication and encryption and security best practices;
- building security into software from the ground up;

- requiring baseline incident response capabilities;
- enabling better endpoint detection and response systems to detect malicious activity; and
- creating event logging so that incidents can be better detected and mitigated.

While it pertains specifically to federal networks, in taking a bold step to chart a new course, the order encourages "private sector companies to follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents."

Given the numerous deadlines established by the order, the coming days and weeks could see an unprecedented amount of activity in the development of cybersecurity standards.

ALIGNMENT WITH BASIC CYBERSECURITY STANDARDS

The Colonial Pipeline incident and the events and announcements discussed above shed light on how organizations can prepare for, and respond to, ransomware and other cybersecurity incidents that involve similar attack vectors and unauthorized access by cyber criminals. While the Executive Order is still being analyzed and further guidance will be provided, one thing is certain: lessons learned must be implemented.

As baseline requirements, organizations should at a minimum do the following to keep pace with the expanding cybersecurity legal obligations:

- Refine your Cybersecurity Incident Response Plans (IRP)
    - An IRP should include detailed response processes that articulate communication, documentation and evaluation activities.
    - For example, the NIST Computer Security Incident Handling Guide has 20 recommendations for an incident response plan.
- Reassess your Cybersecurity Risk Assessment (RA)
    - Certain statutes and regulations mandate RAs and provide guidance and tools to assist organizations.
    - For example, conduct an assessment to analyze your alignment with industry standards and ensure vulnerabilities targeted by ransomware have been addressed.
- Refocus your Written Information Security Program (WISP)
    - Check to see if your WISP includes updated administrative, technical and physical safeguards, as some states now require.

- For example, evaluate and adjust your program in light of any changes to your operations or business arrangements.

Just as organizations continue to embrace digital transformation – the process of leveraging technology, processes and people to innovate – so too will cybercriminals seek to exploit vulnerabilities for big paydays. Today it is ransomware, but tomorrow the attack vector could be new variants or something entirely different (e.g., deep fakes, disinformation, disruptionware, vulnerabilities within IoT devices). Thus, organizations must continue to evolve just as their cybersecurity legal obligations continue to evolve.