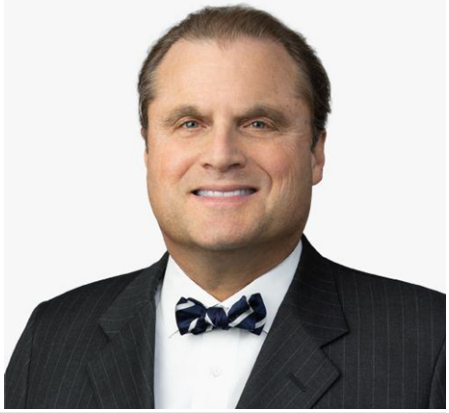
AGENDA

OPINION

The Governance Lessons of the Colonial Pipeline Ransomware Attack

By Michael Peregrine June 1, 2021



Michael Peregrine

Michael W. Peregrine, a partner at McDermott Will & Emery LLP, advises corporations, officers and directors on matters relating to corporate governance, fiduciary duties, and officer-director liability. His views do not necessarily represent the views of McDermott Will & Emery or its clients.

Corporate boards across industry sectors will benefit from reviewing an energy company's recent, controversial choice to accede to the ransomware demands of cyber hackers. It provides an important governance teaching moment on the multifaceted challenges to decision-making under the pressures of a targeted cyberattack.

Ransomware is a form of malicious software designed to block access to a computer system or data by encrypting data or programs on information technology systems. Following a successful attack, hackers extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. This extortion scheme has evolved and now increasingly entails stealing large quantities of sensitive data, which, if the ransom is not paid, are released on the dark web.

Ransomware attacks are becoming more frequent, targeted, sophisticated and — for their victims — costly. Few industries are spared the risk. And one of the more recent, prominent attacks involved Colonial Pipeline, a little-known but crucial pipeline system that provides approximately 45% of the fuel for the East Coast.

Colonial was struck with the ransomware attack in early May, and the ripple effects hit consumers shortly thereafter. Colonial made the difficult decision to pay the $4.4 million ransom given the uncertainty of the scope of the system breach and the larger public in-

terest in avoiding a shutdown of such a critical part of the country's energy infrastructure. To pay the ransom was a highly controversial decision for which Colonial received substantial criticism.

Indeed, the FBI has taken a strong public stand against companies' paying such ransoms. "Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity," the FBI says on its website. In addition, the Department of Treasury's Office of Foreign Assets Control has warned of the sanctions risks to companies and individuals that facilitate ransomware payments to cyber actors on behalf of victims. And, of course, some corporate stakeholders may also take a dim view of ransomware payments made by companies in which they own an interest.

And there's little likelihood of ransomware's diminishing; it can be a profitable business for cybercriminals. Recent news reports indicate that the Colonial Pipeline hackers were able to extort some $90 million in approximately seven months.

So, there's much at stake when the corporate board is faced with a ransomware demand. The time constraints, the threat to operations, the concerns with legal compliance, the sensitivity of data that might be publicly released and the public interest can combine to destabilize the board's traditional decision-making process.

Boards can better prepare to meet these challenges through a series of commonsense steps.

As to process, assure that the right people are "in the room," including board leadership, the general counsel, the chief compliance officer and the chief information security officer, and proactively rehearse ransomware and other cyberthreat scenarios. As to education, familiarize the board with the FTC's five key recommendations for instilling a culture of security within the organization — and act on them. As to risk mitigation, assess insurance options and confirm that ransomware payments and other breach-related costs are covered. As to compliance, evaluate the need to promptly disclose the attack to, and cooperate with, applicable law enforcement agencies and government regulators. As to decision-making, avoid rigid or dogmatic principles ("we never pay criminals") and fully consider the interests of all company stakeholders.

These and similar preparations will help document the exercise of informed business judgment, reducing the risk that officers and directors leading the ransomware response will themselves become part of the controversy.