Lowenstein Sandler

The Tech Group
White Collar Criminal Defense

May 18, 2021

Colonial Pipeline Ransomware Event Highlights Need for Crisis Management Plan

By Kathleen A. McGee and Ken Fishkin

The recent Colonial Pipeline ransomware event provides a strong incentive for organizations to evaluate their resiliency to cyberattacks. With ransomware being the No. 1 concern for many Security Officers surveyed in a recent global poll[1], it is clear that the time for resiliency planning in the event of a cyberattack is immediate. Whether you are designing an initial resiliency plan or updating your organization's current plan, there are several proactive practices you can take to minimize your company's downtime after an attack.

The first step to prepare an organization for an unexpected cyberattack is to conduct "tabletop" exercises with your business units, the IT department, and senior management. Effective and routine workshops highlight the strengths and weaknesses within an organization and can help build a roadmap toward resiliency. Common weaknesses identified during these workshops include inconsistent security awareness training programs, insufficient cyber insurance policies, and inadequate data backup strategies.

Once these technical and nontechnical weaknesses have been adequately identified, one can start developing the organization's Cybersecurity Crisis Management Plan (also known as an Incident Response Plan). The Crisis Management Plan addresses the key phases of crisis response, which include identifying the attack, containing the ransomware or malicious software, removing the software, and recovering from the event. The Crisis Management Plan also details key organization personnel roles and responsibilities during each phase of the plan, as well as points of contact both inside and outside the organization, such as external counsel, customers/clients, vendors, state and local authorities, and potential regulatory agencies.

Once implemented, the Cybersecurity Crisis Management Plan becomes the organization's playbook for addressing various forms of cyberattacks, which in turn ensures a greater of level of resiliency as well as a level of comfort for senior management knowing that their organization has a plan in place for handling a potential ransomware attack.

---

[1] *See* Danny Palmer, ZDNet, *Ransomware is now the biggest cybersecurity concern for CISOs*, Jan. 21, 2021, https://www.zdnet.com/article/ransomware-is-now-the-biggest-cybersecurity-concern-for-cisos/.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

KEN FISHKIN
Manager of Information Security
T: 973.422.6748
kfishkin@lowenstein.com