O'Melveny

Alerts & Publications

Recent Cyber Attacks on Critical Infrastructure Highlight Emerging Cyber Risks in the Water Industry

June 10, 2020

KEY CONTACTS

Matt Kline
Century City
D: +1-310-246-6840

Lisa Monaco
Washington, DC
D: +1-202-383-5413

John Dermody
Washington, DC
D: +1-202-383-5306

Jonathan Yang
Los Angeles
D: +1-213-430-7892

The significant uptick in telework and spear phishing attacks related to COVID-19 has sparked a well-deserved focus on the cybersecurity of information technology networks. A recent high-profile attack against water systems in Israel is a reminder that companies should also be mindful of the cybersecurity threats facing operation technology (OT) and industrial control systems (ICS). Although regulatory frameworks addressing cybersecurity in critical infrastructure are still nascent, companies can prepare now for the operational, reputational, and litigation risks to come.

Israeli officials recently confirmed that a cyberattack earlier this year on its water system attempted to alter the injection of treatment chemicals to unsafe levels. Media reports attributed this activity to Iranian cyber actors, and in May the Iranian port of Shahid Rajaee suffered a significant cyberattack, causing significant disruption of port traffic. Although there has not been official attribution, Israel is reported to be behind the attack.

In May, the President issued an Executive Order on Securing the United States Bulk-Power System that allows the Secretary of Energy to prohibit the acquisition of certain foreign equipment (our prior alert here). While the bulk-power order focuses on only one sector of critical infrastructure, it reflects the increasing concern by government cybersecurity officials with cyber threats to critical infrastructure.

Adding to this recent flurry of activity, on May 28 the National Security Agency (NSA) released a cybersecurity advisory warning that the Russian advanced persistent threat (APT) group known as Sandworm was exploiting a vulnerability in email transfer software. Sandworm is the APT group responsible for the devastating 2017 NotPetya attack and has a history of targeting ICS.

Our teams advise many major financial institutions and other companies in preventing and responding to a range of cyber threats, including the kinds of attacks on information technology systems, including ransomware, that have befallen hospitals, corporations, and city governments in recent years. Such attacks are also targeting utilities and other municipal agencies, and earlier this year, an international cyberattack disrupted the payment system of Greenville Water in South Carolina.

As cyberattacks increasingly venture beyond information technology systems to interfere with basic infrastructure, water systems of all kinds will be exposed to greater operational, reputational, and legal risk:

- Major users and managers of water—including non-utilities such as agricultural producers, industrial operations, and overseers of major campuses or developments—may increasingly face legal exposure for failing to mitigate downstream impacts to their customers and supply chain resulting from a cyberattacks.
- Investors looking to incorporate water assets into their portfolio, or whose investment targets rely heavily on water supply and quality for their business operations, should take care to evaluate the impact that cybersecurity risks may have on the value of a potential investment.
- As adoption of digital technologies in the water industry brings more data and physical systems online, innovators must track and assess evolving risks alongside these new opportunities.
- Commercial insurers may resist coverage for cyberattacks or insist upon reasonable cybersecurity measures.

As seen in other industries, the dramatic impact of a successful cyberattack can suddenly accelerate regulatory responses and resulting legal exposure. Developing appropriate prevention and response strategies requires not only implementing technical security measures, but governance and crisis management plans to manage legal and reputational risk.

Our experienced cybersecurity practitioners continue to advise a wide range of clients facing the growing scope and sophistication of cyberattacks, and together with our wide-ranging Water Practice are available to help industry leaders anticipate and prepare for emerging cyber risks across the water industry.
