Bond Case Briefs

Municipal Finance Law Since 1971

Ftich: Operational Technology Cyberattacks Are a Credit Risk for Utilities

Fitch Ratings-Chicago/Toronto/Austin/New York-23 May 2022: Cyberattacks on industrial control systems/operational technology are more likely to have a credit and ESG impact than a corresponding attack on IT, Fitch Ratings says. Operational technology (OT) systems are vital production technologies that prioritize product or service availability and human safety and are often found in critical infrastructure environments. Cyberattacks that cause prolonged disruption in the delivery of these goods and services and materially affect cash flow, compromise safety or expose governance weakness could be a credit negative.

In the special report U.S. Cyber Risks in Operational Technology (How Operational Technology Influences Cyber Risk for Critical Infrastructure), we explore the IT/OT challenges in the power and utilities and water and sewer sectors, which have been recent targets of cyberattacks. The heatmap below illustrates a breakdown of Dragos' four key findings by OT industry vertical. The report also discusses credit and ESG impacts of cyber incidents in these sectors.

Historically, IT and OT systems were physically segregated and attacks on OT systems were rare; however, IT and OT systems are converging to leverage bigger data sets in real time to optimize performance, costs, safety, uptime and system efficiencies. These convergences, if done correctly, can greatly enhance operations and resiliency, but when done incorrectly, can weaken both operations and resiliency. An attacker that moves laterally and elevates privileges on an OT system can create much more harm compared with an intrusion into an IT system.

Attacks on OT are increasing in both frequency and severity. A report from Claroty found industrial control systems' vulnerability disclosures grew 110% over the last four years and saw a 25% increase in 2H21 compared with 1H21. A report from Ponemon calculated the average cost of a cybersecurity incident to be $3 million and take an average of 316 days to detect, investigate and remediate.

Mon 23 May, 2022