Bond Case Briefs

Municipal Finance Law Since 1971

Moody's: Cyberattacks Could Cause Significant Financial Disruption for Hospitals.

Cyberattacks pose a greater fiscal and credit risk to nonprofit hospitals than any other sector of municipal finance due to the increasingly interconnected nature of hospital operations and information technology.

Hospitals with strong risk management strategies will be better positioned to respond to these operational and financial disruptions, according to a report from Moody's Investors Service.

Small hospitals face the biggest risk, because many lack the necessary cybersecurity resources and will be less able to absorb any financial impact, according to report authors Jennifer Barr, a Moody's analyst, and Lisa Goldstein, Moody's associate managing director.

According to the assessment, the not-for-profit hospital sector's overall cyberrisk is high. Other sectors that have high overall cyberrisk are banks, securities firms and market infrastructure providers because they also rely heavily on technology for their operations.

Data breaches have become a reality for healthcare organizations due to the value of protected health information. In the most critical cases, these data breaches endanger revenue, posing a material risk to financial performance.

To date, Moody's-rated hospitals, representing $250 billion in rated debt, have had sufficient financial resources to absorb the impact of a cyberattack. So far, those impacts have been limited to paying fines when patient data are compromised, with minimal disruptions to operations.

But that could change as cyberthreats evolve and become more sophisticated. Security incidents that result in operational disruptions, like ransomware, present the greatest risk to hospitals, and those disruptive attacks are on the rise, according to Moody's.

Such attacks compromise patient care and expose hospitals to financial losses and lawsuits. Connected medical devices such as insulin pumps, defibrillators and cardiac monitors as well as hospitals' electronic medical record (EMR) systems are points of potential infiltration. Efforts to improve interoperability between organizations, devices and vendors will likely increase this risk, Moody's said.

As the industry continues to push toward digitalization and increased data sharing, the number of infiltration points for cyberattacks will grow.

"Among the biggest risks are attacks against connected medical devices such as insulin pumps, defibrillators and cardiac monitors, which are now entrenched in remote monitoring and require constant updating and patching," the report authors wrote. "The biggest issue for hospitals will be threats that jeopardize patient safety and result in harm or death, exposing hospitals to malpractice accusations and lawsuits."

Ransomware and cyberattacks that compromise hospital electronic health record systems will cause the greatest disruption, affecting hospitals' revenue cycles and disrupting cash flow in the most severe cases, according to the report.

The 2016 ransomware attack at Hollywood Presbyterian Medical Center in Los Angeles had its EMR compromised for several days, resulting in the hospital paying a $17,000 Bitcoin ransom to release the network. The 2017 WannaCry cyberattack on U.K. hospitals resulted in a major IT disruption, causing diversions and delays or cancellations in patient care.

As a result of these threats, hospital management will feel pressured to allocate more resources to protect data and limit system vulnerabilities. Currently, less than 6% of an organization's IT budget is allocated to cybersecurity, according to the Healthcare Information and Management Systems Society. As cyberrisk becomes increasingly important, hospitals will likely increase their investments to shore up cybersecurity programs.

Hospital management teams are developing contingency plans and employing dedicated cybersecurity staff to address threats. Risk management measures include contingency planning, disaster response and obtaining cyberinsurance.

The capacity to take these steps, however, will vary across the hospital sector.

"Small hospitals, particularly critical access hospitals, that lack the resources for a dedicated cybersecurity expert will be more vulnerable. A lack of qualified talent will also remain an industry challenge and require additional investment, leaving less room for investment in other operational areas," the report authors said.

While risk management strategies will help mitigate operational and financial disruptions, malpractice and other legal issues will still be a risk when there is patient harm, Moody's said.

Hospitals remain vulnerable given the overall complexity of their systems and of healthcare delivery as well as the increasing number of attacks.

Fierce Healthcare

by Heather Landi | Sep 12, 2019 3:47pm