Bond Case Briefs

Municipal Finance Law Since 1971

S&P: Cyber Risk Management For U.S. Municipal Utilities Should Be Routine And Requires Vigilance And Flexibility

Key Takeaways

- Developing a cyber defense framework should now be an essential part of risk management planning for U.S. municipal water and wastewater utilities.
- By preparing plans in advance, utilities can ensure continuity of delivery if a cyber incident occurs.
- During a cyber incident, utilities must maintain clear communication with their customers and the general public explaining what is happening and what they are doing about it.
- Recovery planning could generate liquidity problems if not addressed in advance.

S&P Global Ratings believes that cyber risk is an important factor to consider when evaluating credit and has become a key credit focus of risk management for many U.S. municipal utilities. The threat to organizations and the credit impact could get worse before it gets better with the prevalence of cyber breaches and the growing sophistication of cyber criminals. Municipal water and wastewater utilities must develop cyber defense frameworks to prepare themselves for such incidents to ensure continuity of delivery, maintain clear communication with their customers, and have recovery plans in place.

Like other local government counterparts, municipal water and wastewater utilities require trust and transparency with their users: trust that the services will be there and transparency to support decisions about rate increases. Improved technology at the plants can aid in strengthening that trust and transparency and has enhanced data collection, streamlined operations, and improved the user and customer experience. Ironically, however, these benefits also make utilities more vulnerable to cyber crime.

These days, it is easy to become a cyber criminal. On the dark web, there are more ready-made tools and programs available to crack passwords or launch malware, some even with money-back guarantees. In our conversations with utility management teams, we regularly discuss preventative measures, but given the accessibility of technological crime tools, we still find that many utilities are reactive, forced to face these issues as they happen with only miminal advance planning on how to respond.

Cyber breaches pose several risks to municipal utilities. These include the loss of financial assets, personally identifiable information being compromised, and infrastructural and organizational disruptions, not to mention the long-term erosion of public trust. Cyber-preparedness is perhaps even more serious for municipal water and wastewater providers due to the critical nature of this resource: Water is an essential service, and the public has an implicit trust and expectation that such critical infrastructure will be protected and the resource will available when needed.

As we noted in “When U.S. Public Finance Ratings Change, ESG Factors Are Often the Reason” (published March 28, 2019 on RatingsDirect), governance and management issues are the most likely factor behind a rating action across U.S. public finance. Even if a particular disruption is not so serious as to genuinely affect credit quality, headline risk can create different but equally challenging headwinds. The effects of controversies such as a cyber breach and the resultant adverse publicity can weaken citizens' faith in local elected and administrative leadership should the attack be handled poorly or multiple attacks occur. Scrutiny of decision-makers and their risk management practices is likely to increase.

If a utility needs to increase operating revenues, its only option is generally to raise rates. An erosion of public trust could make that more difficult. If the management team scales back or delays rate adjustments–regardless of the reason–the financial profile could weaken, thereby reducing capital commitments or pushing them out to later years, ironically creating vulnerability to even more operating risks. Part of our ratings analysis has always included an assessment of the management team's preparedness and resilience in the face of such events and the relative exposure to observable event risks, in addition to ensuring continuity of operations and maintaining financial performance. If, in our view, that becomes diminished after a cyber breach, it very well could be the case that headline risk has a measurable effect on the utility's credit.

To date, losses from cyber breaches have generally been absorbed by the rated entities' available liquidity and have not resulted in a material decline in credit quality. However, as cyber risk evolves so rapidly, it may only be a matter of time before more serious repercussions arise. Negative rating actions have occurred in other sectors due to cyber breaches. Clearly, every dollar stolen is a dollar than could have been reinvested as a capital investment or other system improvement. If a successful cyber attack on a rated entity significantly affected the expenses, revenue collections, and liquidity position or caused an entity to require the need for further debt to recover from the cyber event, there would clearly be downward pressure on the rating.

Preventive Measures Can Feel Like Catch-Up Actions, But Are Critical

Cyber criminals can be more adaptive and flexible in their approach than the existing countermeasures against them. Thus, in many cases, security technology is playing catch-up. Therefore, cyber risk mitigation is actually more of a management and governance challenge than a purely technological issue. Identifying the organizational workings, risks, and needs of a utility is the most important step in developing a cyber defense framework. Management's in-depth understanding of the assets in terms of personnel, data, and the operational aspects of the system is key to identifying areas of risk within the overall utility.

While a number of best practices exist for not only cybersecurity, but also risk management in general, the America's Water Infrastructure Act of 2018 (AWIA) and subsequent Environmental Protection Agency (EPA) rulemaking now compel all utilities serving at least 3,300 people to create–or for some, to update–a vulnerability self-assessment. "Vulnerabilities" include natural disasters but also "malevolent acts" to demonstrate that management has identified risks and how to be resilient when they occur. These plans should address all facets of the utility, from operations to the back office, and are required to be updated every five years. Finally, management must also establish an emergency response plan to show preparedness for identified risks, then certify or attest to the assessment and emergency response plan once submitted to EPA. We believe this is supportive of long-term credit stability, as risk management in general–and cybersecurity specifically–will become a more explicit part of business as usual for nearly all utilities.

Since the nature of cyber crime is constantly evolving, employee training, preparedness, and awareness must also adapt and evolve. The aging of the workforce across the municipal utilities sector and the looming associated retirements pose risks to new managers, who will have work harder to acquaint themselves with the unique challenges of their utility systems and thus create appropriate security countermeasures for their system and their employees. Obsolete or outdated technology and systems also create cyber vulnerabilities for utilities. Therefore, constant monitoring and updating of systems and isolating and maintaining critical operational systems such as SCADA are generally common but essential starting points of a utility’s preparedness planning. Backing up crucial and confidential operational and user data in secure rapid access data storage mediums is another necessary measure. Since the nature of cyber risk is constantly changing, any utility’s preparedness plan should also be flexible and ready to adapt.

Detection of intrusions or anomalous activities is another component in the formulation and maintenance of a utility’s cyber protection protocols. While managers can use technology tools to detect attempted intrusions, these efforts must be coordinated with robust management plans. These tools, coupled with the vigilance of utility operators toward anomalous activities, can make it more difficult for nefarious actors to gain access to utility systems. Detection and blocking of cyber criminals in a utility’s network is extremely important to the organization’s brand and maintenance of its public trust. In our current world of ever-evolving cyber criminals, terrorist organizations, and hostile nation-state actors, municipal utilities pose a tempting target for cyber-crime, cyber warfare and cyber terrorism, where risks are low and rewards are high. The protection of critical water and wastewater utilities is therefore not just a local challenge but also a regional or national security concern.

Response Planning Is Key To Credit Stability

Water and wastewater utilities, being essential service providers, must ensure continuity of delivery in the event of a cyber incident. Thus, response planning is critical for them to be able to operate and maintain the trust of their customers. The implementation of previously well-thought-out action plans and stopgap measures is key to the successful navigation of a cyber incident. Examples of such actions that we have seen include the implementation of emergency supply, preparedness for manual system operations, table-top exercises replicating an attack, and the activation of well-maintained back-up data.

Communication and transparency are also key when responding to cyber incidents. Even during severe cyber incidents, the served citizens’ implicit trust in their governments is underlined by their expectation that critical components (such as water) continue to function. Despite disruptions, cyber attacks should not affect the accountability of utilities to their customers to provide essential services and doing their upmost to maintain the public’s trust and protect personal information. Thus, a robust response plan should include how the breach is represented, how quickly to alert the public, and what management is doing to mitigate the problem. It is also critical for response plans to be regularly reviewed and analyzed to include new approaches and revise procedures in the constantly evolving world of cyber risk.

Recovery Is Easiest When Planned For Before An Actual Attack

Recovery planning is another important component of maintaining public trust in a utility system. It is generally the recovery phase of a cyber incident that poses the greatest credit risk to municipal utilities. The first and foremost credit concern is the cost in terms of damages and resources needed for recovery. The unforeseen costs due to loss of data, compromised systems, recovery consultants(you mean paying them to help after the event?), or deterioration of the affected entities’ liquidity position could pose liabilities, which, in some cases, may pressure credit quality and create uncertainty in the municipal market. So we normally ask utilities about the adequacy of their reserves, liquidity, or rainy day funds when considering their exposure to cyber risk.

The loss of constituent trust is another factor as weak public support may weaken the ability of the affected entity to raise the funds needed to rebalance the system. There may also be calls for the removal in the utility’s management. Therefore, thoughtful response planning is also key to the maintenance of credit quality and public trust for municipal utilities. Response activities must be well coordinated with local and federal authorities and the response plan should include steps regarding communications with them. The lack of response preparedness and transparency in cyber incidents not only erodes public confidence but also makes it more difficult for local and federal law enforcement to track and combat future risks and breaches.

Ultimately, the heightened speed of communication and the rapid globalization of the cyber realm mean that state and local government entities, which previously were only concerned with their local service areas and thus somewhat insulated, are now part of the global risk environment. The importance of these public systems in the fabric of our critical infrastructure, coupled with their limited resources, makes them tempting targets for cyber criminals and other hostile global actors. These factors, coupled with the localized nature of utilities in the U.S., make cyber security a unique operational and credit challenge for water and sewer utilities.

This report does not constitute a rating action.

Primary Credit Analyst: Omid Rahmani

Secondary Contacts: Theodore A Chapman, Geoffrey E Buswick