Bond Case Briefs

Municipal Finance Law Since 1971

Fitch: U.S. Public Finance Cyber Risk Heightened by Geopolitical Conflict

Fitch Ratings-New York/Chicago/Austin/San Francisco-10 July 2025: U.S. public finance issuer cyber risk has risen as a result of the Israel-Iran conflict and greater geopolitical tensions from the U.S.'s recent intervention, Fitch Ratings says. Iranian-state affiliated actors and hacktivist groups are targeting U.S. critical infrastructure, and the frequency of cyber intrusions is likely to rise, as highlighted by joint advisories from the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation, Department of Defense Cyber Crime Center, and National Security Agency.

Previous geo-politically motivated attacks on U.S. public finance entities primarily targeted health care and utilities. New cyber attacks are also likely to take place as distributed denial-of-service and ransomware attacks.

Cyber breaches are known event risks, but the exact timing and magnitude of damages are hard to predict. Following a cyber incident, we assess an issuer's ability to maintain operational continuity, the duration and scale of service delivery interruptions, impairments to cash flows, and reputational damage.

We consider cyber risk under our review of management and governance, where the presence of adequate governance and management is assumed, and weak governance and management may cause the rating to be lower, all other things being equal. Proactive risk management, including robust incident response planning, staff training, vendor oversight, and, if available, insurance is critical for mitigating evolving threats and preserving credit quality in the face of increasingly sophisticated adversaries. Severe breaches that pressure credit metrics or clear deficiencies in cyber risk management can lead to negative rating actions. Historically, most cyber incidents have not resulted in rating actions.

The public sector's increasing vulnerability is evidenced by a history of disruptive high-profile attacks and ransomware campaigns on local governments, utilities, health care providers and transit systems. These cyber incidents have forced temporary suspension of essential services and diversion of resources away from core priorities. The interconnected nature of public finance operations, where multiple agencies and third-party vendors share data and applications, can amplify the effects of a single breach. The growing use of cloud services and remote work arrangements further expand the attack surface, introducing new risks that must be properly managed.

Public finance issuers are especially compelling targets for nation-state adversaries. Low-intensity campaigns or disruptions to essential services such as water, power, health care and transportation can have significant welfare, operational and reputational consequences. Many municipal entities operate with legacy IT systems that may have known vulnerabilities or lack robust network segmentation. Public disclosure requirements mean that much of the financial information for municipal entities is available to cyber adversaries. Attacks on infrastructure like power or water can also create downstream risks for other sectors.

Federal cybersecurity resource reductions such as the one-third reduction in CISA headcount thus far this year could further pressure state and local governmental resilience by inhibiting coordination, defense and response. Resource constraints were already an ongoing challenge for the public sector, with smaller entities often lacking the budget, technical expertise, and personnel to implement robust cybersecurity measures or comply with CISA reporting guidelines for critical infrastructure. Public finance entities increasingly rely on third party vendors and cloud-based solutions for cybersecurity support. Strong vendor risk management is a vital part of any cyber risk mitigation strategy.

Local governments often struggle to attract and retain skilled cybersecurity professionals due to budgetary constraints, competition from the private sector, and a limited talent pool. As a result, municipal IT teams may lack the capacity to implement advanced security controls, monitor networks continuously, and respond swiftly to incidents. These workforce gaps increase the likelihood of successful attacks and amplify operational and financial risks.