Bond Case Briefs

Municipal Finance Law Since 1971

Fitch: U.S. Public Finance Cyber Risk Elevated Due to Iran Conflict

Fitch Ratings-Austin/New York/San Francisco-09 March 2026: U.S. public finance issuers face elevated cyber risk because of the Iran conflict, Fitch Ratings says. Previous geopolitically motivated attacks on U.S. public finance entities primarily have targeted health care and utilities. Increased broad-based retaliatory cyber intrusions also are likely.

The attacks launched by Israel and the U.S. on Iran on Feb. 28 may lead to escalated cyber reprisals against U.S. public finance entities by Iran and its proxies, compared with attacks in summer 2025. Iranian state-sponsored actors, hacktivist groups, and lone-wolf attackers will likely target U.S. public entities and critical infrastructure more frequently. Risks include distributed denial-of-service attacks, financially motivated campaigns, and attacks that seek to cause physical disruption or destruction. Attacks on infrastructure such as power or water systems can create downstream risks for other sectors.

Public finance issuers are targets given the essential services they provide, IT system vulnerabilities, and data collection. Smaller, resource-constrained public finance entities are particularly vulnerable, as federal cybersecurity resource reductions may hinder robust defense, coordination, and response.

Federal authorities have identified Iran-affiliated actors as responsible for a broad array of previous high-tech attacks targeting U.S. infrastructure, typically through networks and internet-connected devices. Federal authorities have also warned that the recent escalation in the Iran conflict could prompt retaliatory attacks by lone-wolf actors.

Following a cyber incident, Fitch assesses a public finance issuer’s ability to maintain operational continuity, the duration and scale of service delivery interruptions, impairments to cash flows, and reputational damage. Proactive risk management, including robust incident response planning, staff training, vendor oversight, and, if available, insurance, can mitigate threats and help preserve credit quality. Severe breaches that weaken credit metrics or reveal deficiencies in cyber risk management can lead to negative rating actions. Historically, most cyber incidents have not resulted in rating actions.

Copyright © 2026 Bond Case Briefs | bondcasebriefs.com