Bond Case Briefs

Municipal Finance Law Since 1971

Fitch Rtgs: Data Breaches Highlight US Public Institutions' Cyber Risks

Fitch Ratings-Austin-09 January 2019: The recently reported data breach at San Diego Unified School District, affecting the personal data of as many as 500,000 students, underscores the heightened threat of cyberattacks that educational, governmental and healthcare organizations face due to the sizable amount of personal data housed on their networks, says Fitch Ratings. Cyber risk is not a driver of credit risk or rating actions. However, our ratings reflect issuers' overall resilience to manage and respond to changes in its operating environment, including risks associated with cyberattacks.

Data breaches in the education, governmental (including federal and military) and healthcare sectors (including private concerns) accounted for about 40% of total data breaches in 2017 and 2018, according to the Identity Theft Resource Center (ITRC). Approximately 27% of total breaches occurred in the healthcare sector. Combined data breaches for these sectors have increased 160% since 2005, with healthcare having the highest attributable growth, while governmental organizations realized modest improvement. The growth of Internet of Things (IoT), interconnected sensors embedded in technology, such as WIFI networks, building maintenance systems, medical devices and traffic sensors, further contribute to cyber risk. IoT devices outnumbered the world's population in 2017 and are projected to double by 2020, according to Gartner technology consultants.

Cyberattacks create service disruptions for educational, healthcare and governmental organizations, adversely affecting their public service missions and resulting in increased costs. Incident response, crisis management, forensic services and restoration can cost millions of dollars for resource-challenged operations. Some organizations have also paid ransomware demands to retrieve data. Public confidence can also be affected if an organization is perceived to lack preparedness or if their response is seen as insufficient. Exposure of personal and sensitive data can lead to direct costs to personal consumers and loss of confidence in public organizations. Fifty-three percent of data breaches during 2017 exposed Social Security numbers and 19% exposed credit/debit card numbers, according to the ITRC.

The Department of Education has suggested that schools conduct security audits and train staff and students on data security best practices to mitigate cyberattacks. However, there are challenges to adopting cybersecurity best practices within schools as laws do not generally mandate comprehensive standards. Furthermore, these activities compete for scarce budget dollars. Governmental resources are available for guidance and support, such as those provided by The National Institute of Standards and Technology (NIST). However, NIST services have been recently curtailed due to the current lapse in governmental funding.

Contact:

Rebecca Meyer, CFA, CPA, CISA
Director, Public Finance

+1 512 215-3733
Fitch Ratings, Inc.
111 Congress Ave., Suite 2010
Austin, TX 78701

Justin Patrie, CFA
Fitch Wire
+1 646 582-4964
33 Whitehall Street
New York, NY 10004

Media Relations: Sandro Scenga, New York, Tel: +1 212 908 0278, Email: sandro.scenga@thefitchgroup.com