Bond Case Briefs

Municipal Finance Law Since 1971

Increasing Higher Education Cyberattacks Add to Financial Pressures: Fitch

Fitch Ratings-Austin/Chicago/New York-05 May 2022: The higher education sector has seen a rapid increase in the number and severity of cyberattacks since 2020, at a time when many of these institutions are already grappling with financial and operating stress related to the pandemic, Fitch Ratings says. The sector is viewed as a target-rich environment due to the large amount of sensitive data, namely intellectual property (IP) and personally identifiable information (PII), that these institutions maintain for student curriculum, research and operations.

Threat actors took advantage of the pandemic to cause disruption to the higher education sector at a time when it was facing unprecedented challenges and a sharp shift to online delivery. Colleges and universities became much more reliant on remote third-party learning platforms and personal student devices to conduct classes, significantly increasing the exposure for these institutions. Insufficient digital infrastructure and network protection protocols can be material vulnerabilities across the sector.

A unique risk facing the sector is the theft of research data and IP by nation-state actors. In the past two years, more than 200 universities publicly disclosed they were victim to this type of theft, according to a 2021 threat intelligence report from BlueVoyant. Attacks targeting medical and biotech research accelerated during the pandemic, although the main target is still industrial and defense technology information. These cyberattacks could result in the loss of competitive grants and future patent royalty revenues, both critical lines of revenue for research-heavy institutions. In cases where staff or researchers are implicated, the risk of legal and financial repercussions are elevated. Federal contracts generally have cyber hygiene requirements with which universities may need to comply in order to conduct research or receive federal funding.

Investment in cyber preparedness is critical, as underfunding will continue to be exploited by bad actors as long as profit incentives remain high and outweigh the perceived risks of criminal prosecution. Institutions with larger financial cushions typically have more flexibility to afford material IT spend to shore up cyber defences or to respond to an attack. However, these costs would place a greater burden on institutions facing pre-existing operating pressures or with limited financial reserves. The average total cost of a data breach in the higher education sector is about $3.9 million, according to a 2020 Ponemon Institute report.

This effect of cybercrime is exacerbated by labor and funding issues. According to BlueVoyant, 77% of sector CIOs listed hiring and retaining IT talent as a top institutional priority that was hindered by uncompetitive salaries. Another two-thirds reported that IT funding has not recovered from budgetary cuts over the past decade. Preliminary Fitch median data suggest that overall capital spending still trails pre-pandemic levels.

Ransomware attacks against universities doubled through 2020, per BlueVoyant, and, together with ransom demands, continue to increase. Ransomware trends, such as double extortion, where attackers do not return access to data and threaten to leak stolen data if a ransom is not paid, are a

critical risk, as college and university databases contain a wealth of sensitive information. Cyber breaches that disclose confidential information carry financial, legal and reputational risks, and the risk of enforcement actions, due to regulations regarding privacy and confidentiality.

In the event of a cyberattack, Fitch would assess the effect on financial metrics and performance disruption to operations and provision of services, delays in revenue generation, ransomware payments or unexpected capital costs. Cyber risk is an asymmetric credit consideration reviewed as part of our assessment of management and governance, where only weaker characteristics may affect the rating and are reflected in an elevated Environmental, Social and Governance (ESG) Relevance Score.

Contacts:

Omid Rahmani
Associate Director, US Public Finance
+1 512 215-3734
Fitch Ratings, Inc.
Hearst Tower
300 W. 57th Street
New York, NY 10019

Emily Wadhwani
Senior Director, US Public Finance
+ 1 312 368-3347
Fitch Ratings, Inc.
One North Wacker Drive
Chicago, IL 60606

Sarah Repucci
Senior Director, Fitch Wire
Credit Policy – Research
+1 212 908-0726

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