Bond Case Briefs

Municipal Finance Law Since 1971

Fitch: Ransomware a Growing Cyber Risk for US Corporates, Financials, Govt

Fitch Ratings-New York/Chicago-27 April 2022: The frequency, severity and sophistication of ransomware attacks in the U.S. rose dramatically in 2021 from the prior year, a trend that is expected to continue as long as profit incentives remain high and outweigh perceived risks of criminal prosecution. While Fitch has not taken credit rating actions in any sector from a ransomware attack, risks are increasingly negative for affected issuers due to rising ransom costs amid increasingly effective extortion techniques, and the increasingly diverse proliferation of attacks given the interdependency of systems and businesses across the supply chain.

In 2021, there were 421.5 mil. attempted ransomware attacks in the U.S. and 623.3 mil. globally, up 98% and 105% YoY, respectively, according to a March 2022 report from the Senate Committee on Homeland Security and Governmental Affairs. Ransom payments are also increasing; for 1H21, financial institutions reported $590 million in ransomware payments, exceeding all payments made in 2020.

Cybercrime has increased since the pandemic as businesses expanded their remote access capabilities and digital footprints. According to the Senate report, ransomware attacks on government entities outpaced attacks on the private sector. Sectors such as healthcare and financial services that possess valuable personal sensitive information, payment data or intellectual property tend to be targeted most.

Cyber criminals indiscriminately targeted high-value organizations with substantial financial resources and increasingly small-medium-sized enterprises across the globe throughout 2021. Cyber criminals are increasingly utilizing denial of service (DoS) and other burgeoning extortion techniques such as ransomware-as-a-service (RaaS) and are continually rebranding to evade law enforcement. The stealing and encrypting of sensitive personal data in double- and multi-pronged extortion attacks have also grown dramatically. These attacks often occur by utilizing leak sites on the dark web with the threat of releasing of sensitive data and personal information.

Increased incidents have led to executive orders and proposed legislation to address these risks. There were also several high-profile arrests within several ransomware groups and some even claiming to have shut down, even if temporarily. In the U.S., the Cybersecurity and Infrastructure Security Agency (CISA) has mandated minimum hygiene levels and the FBI patched vulnerable servers via a court order. The SEC recently proposed new rules for enhanced and standardized cybersecurity incident reporting disclosures by publicly traded companies within four business days of the event.

These positive steps are additive, with potential material benefit from increased levels of transparency regarding cyber risk, and the elevation of these risk concerns to the board and executive levels. This is critical as boards establish budgets for risk management, but more importantly approve risk parameters and choose leadership that establishes risk culture.

Fitch will review any reported, known or identified cyber incident individually, assessing the effects of a cyber event relative to ratings headroom and financial, operational and reputational impacts. As cybersecurity is an asymmetrical risk, Fitch does not give credit for favorable cyber hygiene and risk management, but deficient cybersecurity management can adversely affect ratings.