PERSPECTIVES

WHY MUNI INVESTORS SHOULD CARE ABOUT CYBERSECURITY

May 28, 2019
By Alriona Costigan and Jesse Starks

Baltimore continues to dust itself off after a May 7 ransomware attack that shut down most of its servers and knocked the city's operations sideways.[1] The attack crippled various systems that collect revenue for the city, such as parking fare databases and housing permit payment systems. The city remains unable to send or receive emails from its city accounts, and many of the city's employees—in particular those processing permits for property sales—are unable to efficiently do their jobs despite a manual *workaround* launched last week.

The city's inability to process property sales is a credit issue for the city. Baltimore general obligation (GO) bonds—like many local GO bonds—are backed by the value of local real estate, via property taxes. Property tax makes up just under half of Baltimore's general fund revenues. The May cyberattack on Baltimore followed another that occurred in March 2018, when hackers breached the city's 911 system. That attack threatened public safety in the city and increased its ESG risk profile.[2,3]

Baltimore's experience underscores the fact that cyberattacks are a growing municipal credit risk. Baltimore follows high-profile attacks in 2018 in Atlanta, where a ransomware attack cost an estimated $17 million or about 2.6 percent of the city's budget; in 2016 in Lansing, Michigan, where upgrading computer systems cost $2.5 million, or 7 percent of revenues; and other incidents.[4,5,6] The rising prevalence of cyberattacks was recently highlighted in a study by the Massachusetts legislature which revealed 26 million attempts to gain access to state systems in a one-hour period between 1 AM and 2 AM on September 13, 2018.[7] Moody's Investors Service noted that at least 24 ransomware attacks on regional and local governments have been reported so far in 2019.[8]

AN ESG RISK

In our view, cyber risk is best captured in credit analysis via the integration of environmental, social and governance (ESG) analysis. We believe poor cyber-risk mitigation can suggest weak governance and threatens to erode public confidence in a government's competence.

Cyberattacks can hurt issuers' reputations, evidenced by the fact that many cities and states avoid reporting them.[9] Voters may say they don't trust leaders who poorly manage cyber risk. However, the lack of consistent reporting of cyberattacks could leave many issuers complacent about the risks or unaware of some of their own vulnerabilities.

Data breaches also present particular risks for hospitals and other healthcare facilities. Medical records can be sold, impacting patients' mental health and security. In 2017, over half of the reported breaches occurred at healthcare, medical provider and medical insurance services organizations, according to the *Privacy Rights Clearinghouse*.

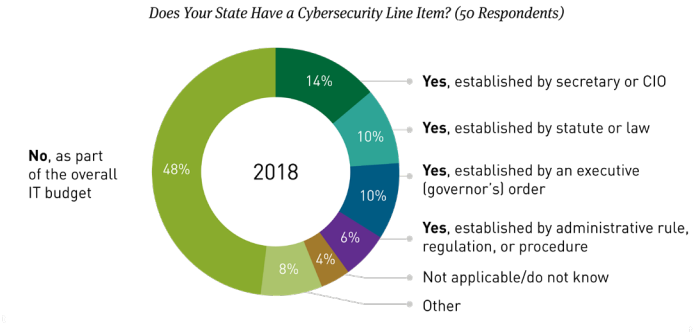
HIGHER RISK FOR SMALLER AND CASH-STRAPPED GOVERNMENTS

While cybersecurity is a credit risk for all municipalities, cyberattacks could have even more deleterious effects on smaller state and local government issuers, which may have less funding to dedicate to strong defenses or preparedness. Also, these smaller issuers may have less incentive to put funding into cybersecurity versus larger cities or states, which may have bigger pools of sensitive data or more online systems that could significantly impact operations. Ransomware criminals may see smaller school districts or towns as easier targets, as their focus on cybersecurity is less than that of larger cities such as Los Angeles, which has a cybersecurity working group in place.

As illustrated by Figures 1 and 2, state spending on cybersecurity is increasing, but only slowly. Only 14 percent of states have a separate budget line item for cybersecurity. Cybersecurity budgets compete with unmet funding needs

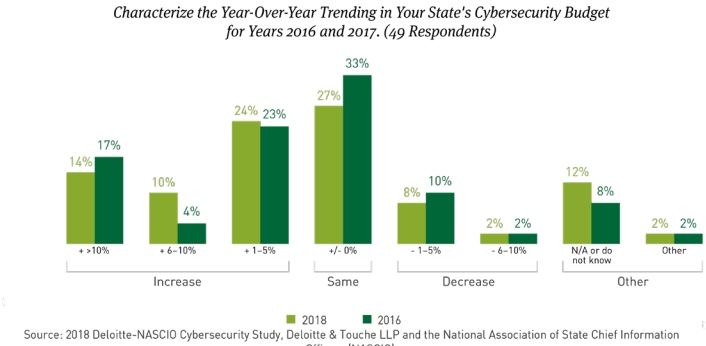
for pensions, other post-employment benefits (OPEB) and aging infrastructure. State and local pay scales are also generally much lower than in the private sector when it comes to attracting cyber talent.

FIGURE 1: ALMOST HALF OF STATES DO NOT HAVE A SEPARATE BUDGET LINE ITEM FOR CYBERSECURITY



Source: 2018 Deloitte-NASCIO Cybersecurity Study, Deloitte & Touche LLP and the National Association of State Chief Information Officers (NASCIO).

FIGURE 2: CISO BUDGETS ARE GROWING SLOWLY; COMPARED TO 2016, ONLY AN ADDITIONAL TWO STATES HAVE REPORTED A BUDGET INCREASE



Source: 2018 Deloitte-NASCIO Cybersecurity Study, Deloitte & Touche LLP and the National Association of State Chief Information Officers (NASCIO).

BETTER DISCLOSURE IS A KEY TO BETTER ANALYSIS

Given the potentially significant impacts of cyberattacks, cybersecurity risks are growing in importance for municipal analysis. Improved disclosure can go a long way toward providing investors with the information they need. For investors, the first step is to determine whether the top leaders of a state or local government take cybersecurity seriously as a risk to operations. This may be reflected in published security policies and/or disclosures in preliminary official statement (POS) documents for new municipal deals. It is also important for issuers to assess and share with investors the defenses that are in place against cyberattacks. This might include controls against malware, phishing, policies for password management, plans for employee training, or third-party assessments or certifications that demonstrate strong security governance. Resources are available to guide organizations through this process, such as the *CIS Controls*, which is a 20-item checklist of some of the most effective security practices, or *NIST CSF*.

The second step is for investors to look for some disclosure of what the issuer would do in the event of a cyber attack. Even the most ironclad technological and physical defenses can be breached, so preparedness for cyberattacks is important to assess as a credit issue. Preparedness can be evaluated by various criteria, such as the presence of a written response plan for an attack, the size of the cybersecurity budget, the presence of insurance against attacks and the strength of the disaster-recovery plan. Notably, the Lansing water system mentioned earlier used cyberinsurance to cover its cyberattack expenses.

Disclosure is improving, but in our view there is a long way to go. At Breckinridge, we are mindful of growing cybersecurity risks and their impact on issuers.

Thus, cybersecurity criteria is incorporated into our analyses of governance and long-term planning for municipal issuers. We look to issuer reporting for data on some cybersecurity criteria. For example, in recent bond offering documents, state and local government issuers have disclosed details on IT training, incident response plans and cyberinsurance. However, we may also ask questions related to cybersecurity during our municipal engagement calls (see *Municipal Engagement Yields Additional Insights*).

As cybersecurity matters continue to increase in importance to issuers, we will continue to integrate the criteria into our municipal research approach.

FOOTNOTES:

1. Scott Calvert and Jon Kamp, "Cyberattack Hobbles Baltimore for Two Weeks and Counting," *The Wall Street Journal*, May 21, 2019.
2. Kevin Rector, "Baltimore 911 dispatch system hacked, investigation underway, officials confirm," *The Baltimore Sun*, March 27, 2018.
3. ESG risk profile according to Breckinridge Capital Advisors analysis, as well as third-party organizations such as MSCI.
4. Atlanta, Georgia FY 2019 adopted budget, *https://www.atlantaga.gov/home/showdocument?id=38261*.
5. Stephen Deere, "Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million," *The Atlanta Journal-Constitution*. August 1, 2018.
6. Rebecca Smith, "How a U.S. Utility Got Hacked," *The Wall Street Journal*, December 30, 2016.
7. Per comments made by Commonwealth of Massachusetts Chief Information Officer and Chief Information Security Officer Dennis McDermitt, Boston, Massachusetts, September 13, 2018.
8. Moody's Investors Service Credit Outlook, May 27, 2019. "Second ransomware attack in 15 months disrupts Baltimore's operations." U.S. Public Finance.
9. Alex Dobuzinskis and Jim Finkle. "California hospital makes rare admission of hack, ransom payment," February 18, 2016. Taken from *https://www.reuters.com/article/us-california-hospital-cyberattack/california-hospital-makes-rare-admission-of-hack-ransom-payment-idUSKCN0VS05M*.