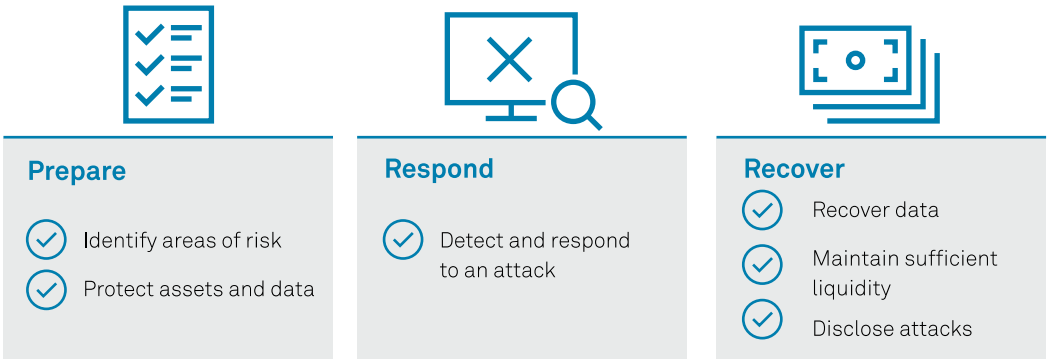
# ESG Brief: Cyber Risk Management In U.S. Public Finance

**June 28, 2021**

### What We're Watching




Source: S&P Global Ratings.


As cyberattacks increase in sophistication and frequency, U.S. public finance (USPF) issuers must embed cybersecurity into their comprehensive risk-mitigation strategies. We consider risk management and mitigation a governance factor under environmental, social, and governance (ESG). We believe most municipal issuers' preparedness will support credit fundamentals and prevent significant financial or reputational fallout that could result from an attack. In our view, all USPF issuers should be taking steps to mitigate their exposure to event risk stemming from a cyberattack. An inability to fully restore operations in a timely manner after a cyberattack could lead to rating pressure. USPF issuers experienced cyberattacks before the COVID-19 pandemic, and we have been analyzing potential credit impacts for more than half a decade (see Related Research below). Our analysis of an issuer's strategy to prepare for, respond to, and recover from an attack uses the National Institute of Standards and Technology (NIST) standards as a benchmark for a sound plan, as it has since cyberattacks first emerged as a credit risk several years ago. However, the universe of USPF issuers is broad and diverse and the NIST framework, first established in 2014 and updated regularly, is very detailed and focused on protecting critical infrastructure. Therefore, our analysis of an issuer's preparedness and mitigation practices typically considers the role of the organization as well as the size and scope of its operations since many issuers are not responsible for critical infrastructure elements.

**PRIMARY CREDIT ANALYSTS**

**Tiffany Tribbitt**
New York
+ 1 (212) 438 8218
Tiffany.Tribbitt
@spglobal.com

**Geoffrey E Buswick**
Boston
+ 1 (617) 530 8311
geoffrey.buswick
@spglobal.com

**SECONDARY CONTACTS**

**Nora G Wittstruck**
New York
+ (212) 438-8589
nora.wittstruck
@spglobal.com

**Theodore A Chapman**
Farmers Branch
+ 1 (214) 871 1401
theodore.chapman
@spglobal.com

**Ken W Rodgers**
New York
+ 1 (212) 438 2087
ken.rodgers
@spglobal.com

**Aamna Shah**
San Francisco
+ 1 (415) 371 5034
aamna.shah
@spglobal.com

**See complete contact list at end of article.**

## Prepare: Best Practice Is For Issuers To Include Cybersecurity In Risk-Mitigation Plans

We expect all issuers to have a basic knowledge of their physical and digital assets, including personally identifiable data that may have special legal protection. In addition, we believe issuers should understand where vulnerabilities are in their systems. This understanding typically is documented in a device and network inventory and includes implementation processes to mitigate cyber threats. Furthermore, it includes an understanding of risks from vendors and third-party relationships for information technology, accounting, billing, or other purposes. Understanding what could be at risk is the first step in developing an effective mitigation strategy.

In addition, we expect issuers to take basic steps to protect their assets, such as implementing cyber hygiene practices and staff training. Good cyber hygiene practices include but are not limited to firewalls, antivirus software, multifactor identification requirements, security-patch management, phishing exercises, and email filters. Additional policies, including regular access audits and vendor management, should be implemented, as necessary, based on the size and sophistication of the issuer. Given the rise in social engineering fraud, controls around wire transfers and bank payments should also be in place, as necessary. Finally, for large issuers or those more frequently targeted, such as states, utilities, health care facilities, and higher education institutions, we would expect the issuer to have a dedicated chief information or chief information security officer, or to identify the person or department ultimately responsible for securing assets and data.

## Analytical Considerations – Issuer Preparedness

### All USPF sectors

Issuers unable to properly identify cyber event risks could encounter significant delays in stopping or recovering from an attack, leading to service disruption, additional liabilities such as ransomware payouts or legal issues from data breaches, or other negative effects that could cause rating pressure. Certain sectors face additional heightened risk if they fail to thoroughly assess their risks and create an action plan to follow should an attack occur.

### Electric cooperatives and municipal-owned public power utilities

Given the interconnected nature of the electric grid in the U.S. and its status as both critical infrastructure and highly vulnerable to a sovereign-backed cyberattack, we expect a robust understanding of digitized systems that could be attacked and the downstream impacts an attack could have on operations. This includes understanding if networks are vulnerable to shared risks with state or local governments, or if assets operate on separate networks.

### Water and sewer utilities

Water and sewer utilities are at risk on two fronts: infiltration of operations and potential hijacking of customer account information or municipal financial records. With the precedent set for a cyberattack that can threaten the safety of water supply, we expect water utility operators to understand the risks presented by digitalization of services and operations, with sufficient protective measures in place to prevent life and safety risks following an attack. Failure to do so could lead to significant operational and legal costs, pressuring ratings. Furthermore, industry best practices generally specify that utility operations not be connected to the outside world to limit the risk of an intrusion.

### Not-for-profit health care

With significant amounts of personally identifiable information and medical information subject to HIPAA privacy laws, we expect issuers to have a thorough understanding of retained data and a formidable cyber defense strategy. Failure to have a proper cyber defense strategy and data-management procedures in place is of particular concern for hospitals and health systems as this not only increases the risk of contingent liabilities stemming from data breaches but also jeopardizes the health and safety of patients.

### Higher education

Due to the amount of personally identifiable information collected and retained through the admissions process, fundraising, and the conduct of sensitive research, cyber criminals often view higher education institutions as rich targets. In addition, the huge number of devices on college and university information technology networks creates an expectation that these issuers have processes in place to manage these assets in a secure manner as students and faculty join and leave the system frequently. We believe a well-defined threat matrix is crucial to the identification of information that could be at risk from a targeted attack.

Source: S&P Global Ratings.

## Respond: Best Practice Is For Issuers To Monitor Their Systems And Plan For How To Respond Before An Attack

The longer cyber criminals have access to a system, the more damage they can inflict. Therefore, the ability to rapidly detect an attack could limit damage. At a minimum, we generally expect that issuers have some type of system monitoring to detect a potential threat. This could include a dedicated employee or team, but could also be electronic. The sophistication of the network or a large number of devices potentially exposed would increase our expectation that the issuer has a more advanced governance framework for cyber response.

We also typically expect issuers to consider what they would do in the event of an attack and have a basic plan for data recovery and systems backup. Regular data backups should be part of this plan. For certain issuers, particularly those that provide critical services, we would expect detailed response plans that include exercises to periodically evaluate the effectiveness of the plans using walkthroughs, and tabletop, functional, or full-scale exercises. Failure to have an effective plan could force the issuer to shut down operations, resulting in adverse effects on finances and life and safety. This could lead to a downgrade.

### Analytical Considerations – Ability To Detect And Respond To An Attack

**All USPF sectors**

Failure to detect an attack or respond in a timely manner is often followed by lost revenues and increased costs associated with data recovery. These financial consequences can have negative credit implications. Therefore, if S&P Global Ratings views an issuer's risk management in this area as less robust than that of peers, it could weaken our view of management.

Source: S&P Global Ratings.


## Recover: Preparedness And System Design Can Help Lessen Credit Impact

With the increasing sophistication and constantly changing attack strategies of cybercriminals, absolute avoidance of risk might not be possible. In our view, with proper preparedness and practiced response protocols, damage from a cyberattack could be limited. Recovering from an attack may mean restoring data from backup copies, reconfiguring systems, or using other means of regaining systems access. We also evaluate the sufficiency of an issuer's liquidity to recover from a disruption in its cash flow after a cyber incident. Adequate and available reserves, particularly when supplemented by a cyber insurance policy, usually mitigate this risk. Finally, we look for disclosure of events and impact analysis to ascertain if improvements to risk-management policies and practices might be necessary following an attack. We view a full and timely disclosure following a cyberattack as critical to mitigating potential legal risk from parties potentially injured as a result of the attack, including bondholders. Also, such disclosure can help peers and other municipal issuers better prepare for similar attacks and help the capital markets identify trends and refine best mitigation practices.

### Analytical Considerations – Ability To Recover From An Attack

**All USPF sectors**
Following an attack, we focus primarily on the event's financial impact. Beyond the immediate consequences, we will consider if there are longer-term risks, including contingent liabilities stemming from data breaches or loss of constituent trust that might hinder future revenue-raising capabilities.

Source: S&P Global Ratings.


## An example of cybersecurity embedded in risk-management planning

The example below demonstrates the questions an analyst might ask to assess an issuer's risk-management policies and practices for cybersecurity, with sample answers that would demonstrate risk mitigation for a small local government issuer. Although it's not intended to be a checklist or to apply to every issuer or situation, it can provide a general example of what an analyst might consider when speaking with issuers. Analysts could ask for additional information or look for further policies and practices as the situation warrants.

What steps have you taken to identify and protect your assets and data from cyberattacks?

- Device registration and access controls
- Firewalls, staff training, virus, and malware scans
- Two-signature requirements on wire transfers and payments

What policies and practices have you implemented to enable you to detect, respond to, and recover from a cyberattack?

- Data recovery plans including offsite backups
- Cyber insurance
- System scans to detect malware/attacks
- Ability to isolate attack from affecting entire network

## Related Research

- ESG Brief: Emerging Themes In U.S. Public Finance, June 3, 2021
- Sustainable Finance Newsletter: June 2021, June 14, 2021
- Cyber Risk In A New Era: Disruptions And Distractions Increase Challenges For U.S. Public Finance Issuers, Oct. 19, 2020
- Cyber Risk In A New Era: Remedy First, Prevent Second, Sept. 17, 2020
- Through The ESG Lens 2.0: A Deeper Dive Into U.S. Public Finance Credit Factors, April 28, 2020
- U.S. Public Finance Issuers Must Be Nimble To Fend Off Cyberattacks Or They Could Face Credit Fallout, Feb. 25, 2020

- Cyber Risk Management For U.S. Municipal Utilities Should Be Routine And Requires Vigilance And Flexibility, Feb. 3, 2020
- Blockchain Is Coming To Muniland, And The Changes Could Be Significant, July 30, 2018
- Cyberattacks Pose A Real, If Varying, Credit Risk Across U.S. Public Finance Sectors, Sept. 20, 2017

This report does not constitute a rating action.

## Contact List

PRIMARY CREDIT ANALYST

**Tiffany Tribbitt**
New York
+ 1 (212) 438 8218
Tiffany.Tribbitt@spglobal.com

PRIMARY CREDIT ANALYST

**Geoffrey E Buswick**
Boston
+ 1 (617) 530 8311
geoffrey.buswick@spglobal.com

SECONDARY CONTACT

**Nora G Wittstruck**
New York
+ (212) 438-8589
nora.wittstruck@spglobal.com

SECONDARY CONTACT

**Theodore A Chapman**
Farmers Branch
+ 1 (214) 871 1401
theodore.chapman@spglobal.com

SECONDARY CONTACT

**Ken W Rodgers**
New York
+ 1 (212) 438 2087
ken.rodgers@spglobal.com

SECONDARY CONTACT

**Aamna Shah**
San Francisco
+ 1 (415) 371 5034
aamna.shah@spglobal.com

SECONDARY CONTACT

**Simon Ashworth**
London
+ 44 20 7176 7243
simon.ashworth@spglobal.com