MOODY'S
INVESTORS SERVICE

SECTOR IN-DEPTH
20 May 2021

Rate this Research

Contacts

Heather Correia +1.214.979.6868
Analyst
heather.correia@moodys.com

Orlie Prince +1.212.553.7738
VP-Sr Credit Officer/Manager
orlie.prince@moodys.com

Leroy Terrelonge 1.212.553.2816
Vice President - Senior Analyst
leroy.terrelonge@moodys.com

Lesley Ritter +1.212.553.1607
VP-Senior Analyst
lesley.ritter@moodys.com

Jim Hempstead +1.212.553.4318
MD - Global Infrastructure & Cyber Risk
james.hempstead@moodys.com

Leonard Jones +1.212.553.3806
MD-Public Finance
leonard.jones@moodys.com

» Contacts continued on last page

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

State and Local Government – US

Cybersecurity stronger among larger organizations, including states and transits

To assess US state and local governments' cyber risk preparedness, we surveyed 122 governmental bodies, including states, counties, cities, school districts, utilities and transit authorities. The results show differing degrees of preparedness, with readiness stronger among larger organizations, including states and transit systems, that have access to greater resources. Cybersecurity is an increasing risk for regional and local governments, which have suffered numerous attacks in the past several years. Weak security planning, lax risk prevention or poor response and recovery readiness leave entities vulnerable to attack and are a credit weakness. All observations in this report are based on our survey results and do not represent a definitive assessment of cybersecurity readiness.

» **Larger governments are better positioned to address cyber risks than smaller governments.** States and large transit authorities have developed the most comprehensive response to cyber risk, with local governments lagging behind. Larger entities tend to have greater resources and revenue-raising ability, which allows them to maintain well-rounded cybersecurity practices.

» **Testing an entity's infrastructure for cyber weakness varies widely across sectors surveyed**. System testing for weakness was most common for states and transit systems, with substantial gaps across the remaining cohorts. Positively, most entities adopt other preventive measures, including weekly backups to protect data.

» **School districts trail other governmental sectors in protecting systems and data.** Based on survey results, 86% of districts have incident response plans, but they trail in key metrics such as use of multi-factor authentication and data backups. Advanced and costly cyber risk management practices like "red team testing" are mostly out of reach.

» **Head count and budget allocated to cybersecurity is increasing across most sectors.** Most sectors report increased investment in cybersecurity since 2017, both in the form of additional staff and growing information technology budgets.

» **Most governmental entities have standalone cyber insurance, but our highest-rated issuers are the most likely to carry policies.** Across all sectors, over 60% of respondents report having standalone cyber insurance, with states leading at 76%.

» **Adoption of cloud technology is relatively slow but is likely to grow.** The shift will allow smaller governments that may not have the resources to invest in regular technology upgrades to better protect their assets. Cloud technology can be more secure than hosting data on premise.

How we conducted our cyber risk survey of US state and local governments

To assess state and local governments' cyber risk preparedness, we surveyed 122 governmental bodies, including states, counties, cities, school districts, utilities and transit authorities. The questions covered areas such as governance, including resource allocation; risk management and preparedness, including surveillance and testing methods; and risk transfer, including insurance and cloud adoption.

The survey provided the opportunity to gather consistent feedback on governments' key cybersecurity concerns and responses, helping to identify and define the standards being established across the sector. The survey results also provide a foundation for further analysis of cybersecurity issues and their credit implications.

We present the aggregated survey results as averages for responses to binary, yes-or-no questions (e.g., has your organization developed an incident response plan to respond to cyber incidents?) and medians for responses to nonbinary questions (e.g., how many times a year do you test your incident response plan?).

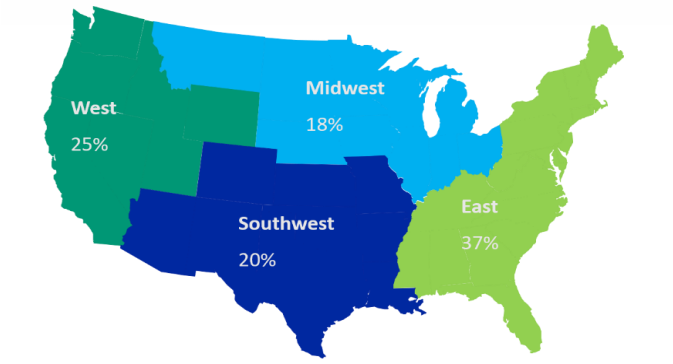
Cyber risk is growing for state and local governments

We view cyber risk as event risk that is growing across all sectors globally, and it is an increasingly important factor in our credit analysis. State and local governments are no exception in this regard. In recent years, local governments have been frequent targets of ransomware attacks; they have lost money through cyber-enabled fraud; and they have experienced significant data breaches. Then, in 2020, the COVID-19 pandemic resulted in a rapid and abrupt move to remote work, creating challenges for managing applications and data outside of traditional networks during a period of increased malicious cyber activity.

In our February 2019 heat map, we determined that the subsectors discussed in this report are exposed to varying levels of cyber risk. The current survey provides a transparent benchmark for how regional and local governments structure their cyber risk governance, management and transfer policies to deal with this rising danger.

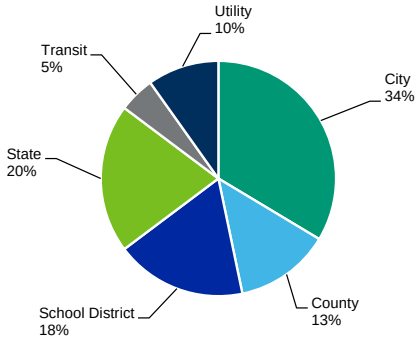
Exhibits 1-4 show the survey respondents by geographic region, subsector, rating, and population size.

Exhibit 1
Survey respondents by geography



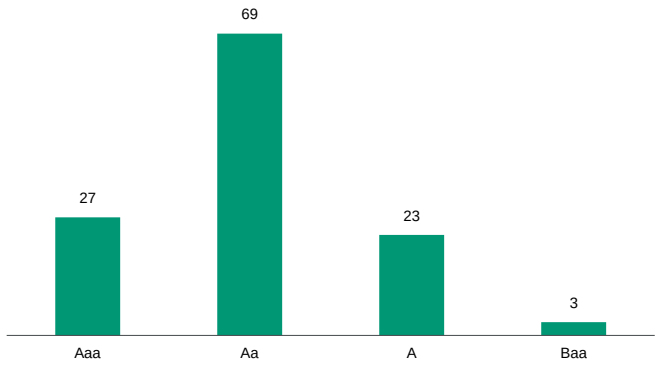
Source: Moody's Investors Service

Exhibit 2
Survey respondents by subsector



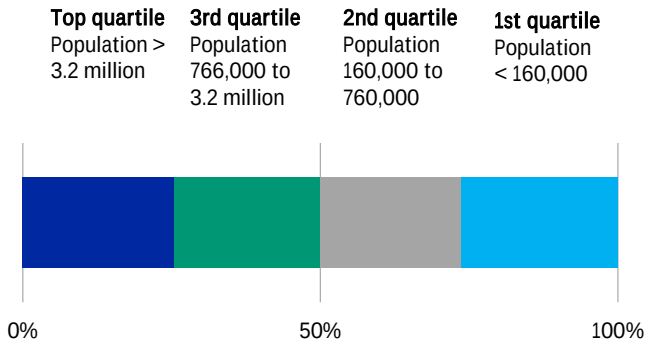
Source: Moody's Investors Service

Exhibit 3
Survey respondents by rating



Source: Moody's Investors Service

Exhibit 4
Survey respondents by population quartile



Source: Moody's Investors Service

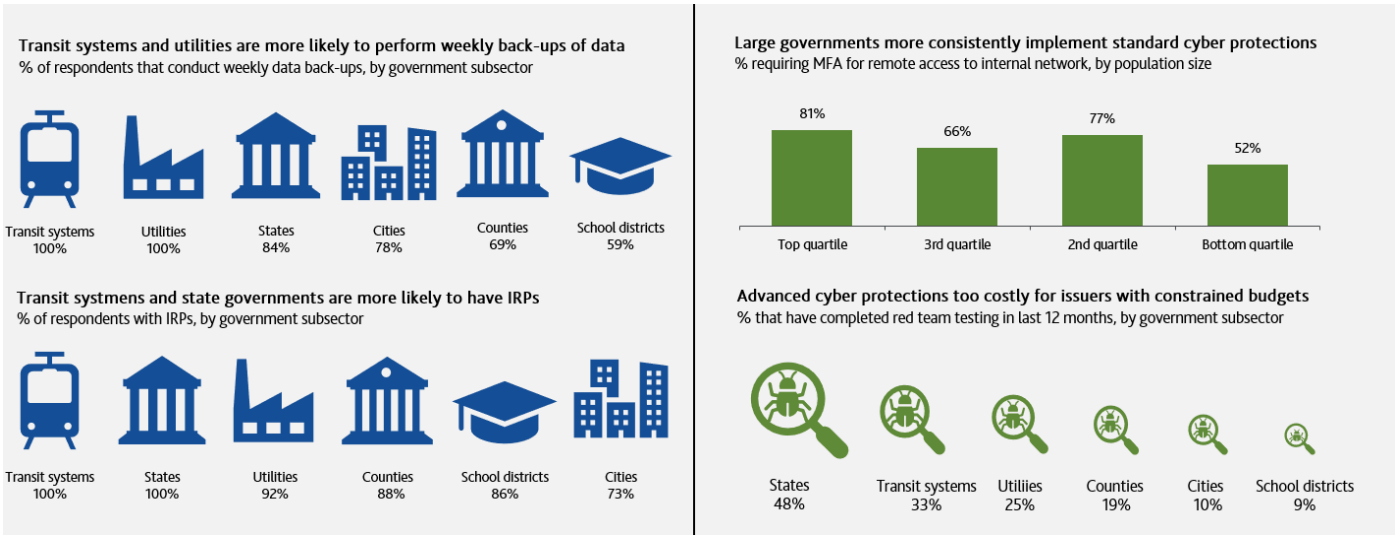
Larger governments are better positioned to address cyber risks than smaller governments

Larger governmental organizations[1], such as states and large transit systems, are in a better position to protect their systems and data than smaller governments, according to the findings of our survey, with entities such as cities and counties lagging behind in their cyber defense efforts. Larger issuers tend to have greater resources and revenue-raising ability, which allows them to maintain more robust cybersecurity practices.

To assess cyber risk preparedness, we asked issuers about their use of four key cyber defense tools: whether they have incident response plans (IRPs) and how frequently these IRPs are tested; whether they use multi-factor authentication (MFA) to access their networks; whether they practice "red team testing," or simulated attacks designed to measure how well an entity could withstand a real-life attack; and whether they conduct weekly data backups.

Exhibit 5 shows how, based on issuers' responses, states and large transit authorities have developed the most complete response to cyber risk. For example, all respondents in these two sectors indicate they have created IRPs that are tested at least twice a year, while 96% of states and 100% of transits use MFA.

Exhibit 5
Larger governments generally make greater use of cyber defense tools than smaller ones



Source: Moody's Investors Service

Local governments, by contrast, lagged behind states and transit systems, with counties leading the way in IRP use at 88%. Use of MFA is also lower. In weekly data backups, too, counties and cities also performed lower than states and transits.

Key tools that governments use to protect their systems and data

Growing awareness of cybersecurity risks has led to the development of new tools and support services to help governments improve their cyber defenses and their ability to recover from potential attacks.

- **Incident response plans (IRPs)** and testing are the foundation of cyber risk management. An IRP is most effective when it is regularly tested, reviewed and updated.
- **Multi-factor authentication (MFA)** is used to manage remote access and is an increasingly important line of defense in light of rapid and wide adoption of remote work arrangements.
- **Data and system backups** remain an effective way to rapidly restore operations when falling victim to a ransomware attack, which typically encrypt a victim's files, until a ransom key is provided by the attacker or the issuer restores its systems using its backups.
- **Red team testing** is an important tool to evaluate an organization's processes, tools and proficiency in responding to different cyberattack scenarios. During a red team test, experts attempt to hack an organization's own systems to identify vulnerabilities and measure how well employees, networks, applications and physical security would withstand a real-life attack.

Testing an entity's infrastructure for cyber weakness also varies widely

The degree to which issuers performed comprehensive testing of their IT infrastructure also varied according to size of government, with states, regardless of size, more likely to carry out red team testing than local governments. Red team testing, while an important tool to evaluate an organization's proficiency in responding to different cyberattack scenarios, can be cost-prohibitive even for entities with ample resources, such as banks. When we surveyed our banking sector, 100% of issuers with over $150 billion in assets reported performing red team testing in the past 12 months. Given this, we would expect most local governments, which generally have far less in reserves than corporate banks, to forgo this type of testing in favor of something less costly – an expectation borne out by our survey results.

Larger governments' greater resources strengthen their cyber risk management, but can boost smaller entities' defenses too

In general, issuers with larger populations and higher revenue had the most robust cyber risk management practices. However, their greater resources and revenue-raising ability not only boost their own cyber defenses, but can benefit smaller municipalities as well. Over the past few years, many states have created cyber response units, usually housed in their technology or Homeland Security department, to help their smaller municipalities in the event of an incident. In both Texas and Louisiana, for example, several small cities and school districts were simultaneously attacked, and each state deployed law enforcement and cyber experts to recover data. Similarly, Ohio created a civilian cybersecurity reserve force to protect local governments, critical infrastructure and businesses from the impact of cyberattacks. Under the law, a local government hit by a cyberattack can ask the governor to deploy the Cyber Reserve (similar to a National Guard) as well as other statewide resources.

School districts lag behind when it comes to protecting systems and data

School districts demonstrated a lower level of cyber risk preparedness than other governmental sectors. Relative to their local government peers, districts trail in key metrics such as MFA use and data backups. Risk management practices such as red team testing, meanwhile, are mostly out of reach for cost reasons, with only 9% of districts conducting them, as shown in Exhibit 6.

Exhibit 6

School districts lag other sectors in terms of cyber preparedness

	School districts	Cities	Counties	Utilities	Transit systems	States
% that have an IRP	86%	73%	88%	92%	100%	100%
Number of IRP updates per year	1	1	1	1	2	1
Number of IRP tests per year	1	1	1	1	2	2
% of online applications subject to a penetration test in the last 12 months	5%	5%	38%	20%	15%	2%
% that have a program responding to external reports of security issues affecting the company's operations or provision of service (i.e. bug bounty programs)	59%	68%	50%	42%	33%	64%
% that have completed red team testing in the last 12 months	9%	10%	19%	25%	33%	48%
% that have a formalized process to address issues found during red team testing	13%	36%	45%	63%	67%	55%
% that use multi-factor authentication for remote access to internal resources	45%	56%	94%	50%	100%	96%
% that back up data and systems at least weekly	59%	78%	69%	100%	100%	84%
% that have completed a tabletop simulation in last 12 months	32%	39%	56%	50%	83%	84%
# of times org engaged with/educated employees on cybersecurity issues in last year (e.g., phishing simulations, awareness campaigns, etc.)	4	4	5	7	15	12

Note: Green represents the strongest performance, and red the weakest. Gray lies between weakest and strongest. This color scheme applies to all charts of this type.
Source: Moody's Investors Service

Unlike other governmental entities that rely on diverse revenue streams (such as income taxes, severance taxes, sales taxes and property taxes), school districts receive a combination of state aid and property taxes, with state aid at the discretion of the legislature. As a result, districts tend to have fewer resources and less revenue-raising ability than other governments. This can hamper their ability to hire industry experts to help them develop a sophisticated approach to cyber protection. Since we began tracking cyberattacks in 2018, the rates at which school districts are targeted (based on yearly aggregate) has increased exponentially. School cyber breaches most often result in unauthorized access to student and teacher data, leaving individuals vulnerable to future misuse of this information, through identity theft for example. Additionally, these attacks can result in school closures or delayed openings. Based on the examples we have observed, if a school does close, it is typically reopened within a week.

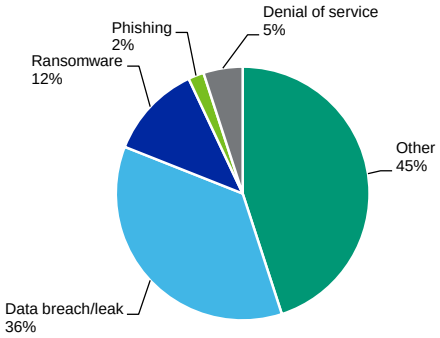
COVID-19 has also had a significant operational impact on school districts across the country because of the shift to a virtual learning environment. Increased reliance on technology and greater levels of connectedness via online devices and virtual services have already led to a sharp increase in cyberattacks on K-12 schools nationwide, as school networks become more attractive to cybercriminals. In 2020, a total of 408 publicly disclosed incidents represented a 15% increase from 2019, according to The K-12 Cybersecurity Resource Center, a website that tracks publicly disclosed cyber incidents at schools across the nation.

Cybercriminals employed a variety of attacks to disrupt district operations, as shown in Exhibit 7. With many school districts having transitioned to virtual learning in the first half of 2020, and likely to maintain it to some extent for the foreseeable future, incidents are likely to rise further.

Exhibit 7

Schools experienced many types of cyber incidents in 2020

K-12 cyber incident types, 2020



"Other" incidents include unattributed malware, class and meeting invasions, email invasion, website and social media defacement, and a wide variety of related/and or low-frequency incidents. The increase in remote instruction as a result of the COVID-19 pandemic led to a jump in class and meeting invasions.

Source: The K-12 Cybersecurity Resource Center, 2020 Report

Injection of federal funds gives school districts an opportunity to boost cyber preparedness

Districts will have an opportunity to increase their investment in cybersecurity since, in response to the coronavirus pandemic, the federal government has allocated significant funding to education. With the Coronavirus Aid, Recovery, and Economic Security (CARES) Act, districts received $13.2 billion in the form of the Elementary and Secondary School Emergency Relief Fund, or ESSER.[2] And with the passage of Coronavirus Response and Relief Supplemental Appropriations Act (CRRSAA), districts are poised to receive another $54.3 billion (ESSER II). These funds must be spent by 2023. The US Congress gave districts considerable flexibility in determining how to use these funds, making it possible that districts will invest in technology upgrades.

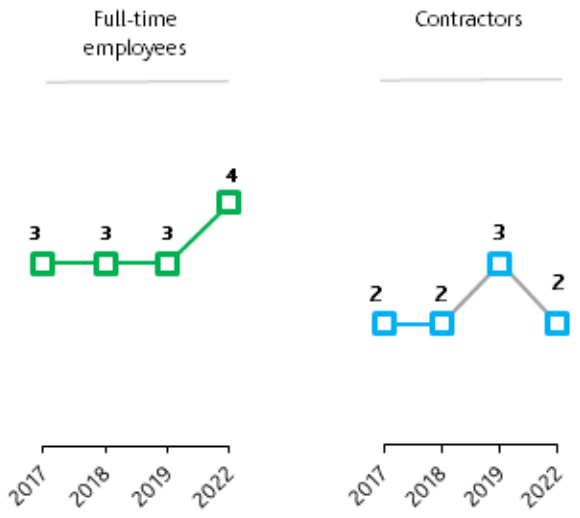
Head count and budget allocated to cybersecurity is generally increasing across all sectors

Despite their limited revenue-raising ability in contrast to the private sector, governments have allocated increasing funds to address cyber risk. Most sectors report increased investment in this area since 2017, both in the form of additional cyber-dedicated employees and growing IT budgets (see Exhibits 8 and 9).

Exhibit 8

Governments typically have limited staff devoted to cybersecurity

Median number of full-time cybersecurity employees and contractors per year

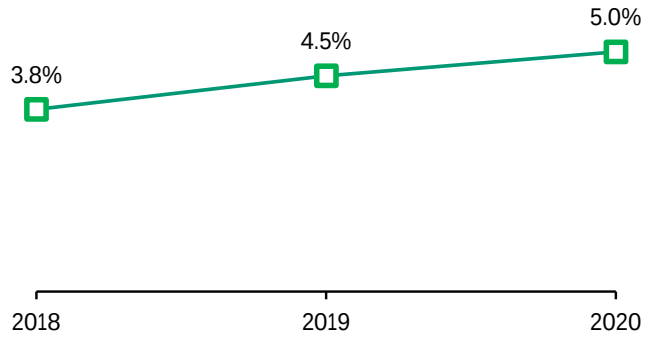


Source: Moody's Investors Service

Exhibit 9

Cybersecurity is consuming a greater portion of governments' technology budgets

Cyber spend as % of tech budget



Source: Moody's Investors Service

Between 2017 and 2019, cities and counties increased their cyber staff head counts by 100%, transits and utilities by 200% and school districts by 300% (see Exhibit 10). Moreover, most sectors intend to increase their staff by 2022, with states – which increased headcount by only 4% in 2017-2019 – reporting they will increase cyber personnel by 86%. While utilities said cyber staff will likely decline by around a third in 2022 to 2 full-time equivalent (FTE) employees from 3, they also plan to increase the number of outsourced positions by 1.5 FTEs, resulting in an overall level head count.

Exhibit 10

Governments are increasing their cyber staff

	School districts	Cities	Counties	Utilities	Transit systems	States
% change in full-time cyber employees (2017 vs. 2019)	300%	100%	100%	200%	200%	4%
% change in full-time cyber employees (2019 vs. 2022)	0%	0%	25%	-33%	100%	86%
% change in outsourced cyber employees (2017 vs. 2019)	0%	0%	100%	100%	133%	150%
% change in outsourced cyber employees (2017 vs. 2019)	0%	0%	100%	200%	43%	300%

Source: Moody's Investors Service

As governments' staffing increases, so do their budgetary allocations. All sectors surveyed, with the exception of states, are allocating greater portions of their IT budget to cybersecurity. And although states appear to trail other governments in the pace of their cyber investments, this is likely not the case. States were early adopters of cybersecurity measures, and developed programs, guidance and teams to assist their municipalities. States are maintaining established cyber programs whereas local governments are now in the process of developing their own – a dynamic that is reflected in the data.

Because of states' size and the resources available to them, their budgets and head counts are far in excess of local governments'. In 2019, for example, counties employed 4 cyber-specific FTEs, the highest of any type of local government. States, by contrast, employed 14.5.

Most governmental entities have standalone cyber insurance, but our highest-rated issuers are the most likely to carry policies

Cyber insurance provides local governments more options in responding to a ransomware attack. While policies vary, they can cover organizations for costs related to paying ransoms, hiring incident responders and purchasing new technology and equipment, which can significantly reduce the costs for victims of ransomware incidents. Exhibit 11 shows that across all sectors, most respondents report having standalone, or dedicated, cyber insurance policies, with states leading at 76% and counties and utilities a close second.

Exhibit 11

Across all sectors, most respondents report having standalone, or dedicated, cyber insurance policies

Cyber insurance usage by subsector, rating and population size

	School districts	Cities	Counties	Utilities	Transit systems	States
% with stand-alone cyber insurance	68%	61%	75%	75%	67%	76%
% with explicit cyber coverage through traditional insurance policy	43%	53%	33%	40%	17%	20%

	Aaa	Aa	A	Baa
% with stand-alone cyber insurance	67%	74%	61%	33%
% with explicit cyber coverage through traditional insurance policy	38%	34%	55%	0%

	Top quartile	3rd quartile	2nd quartile	Bottom quartile
% with stand-alone cyber insurance	63%	76%	80%	58%
% with explicit cyber coverage through traditional insurance policy	28%	44%	34%	47%

Source: Moody's Investors Service

While size of government was not a significant factor in cyber insurance, coverage showed greater variation by rating. Our highest-rated issuers are the most likely to have policies. Across Aaa-, Aa- and A-rated issuers, at least 60% report carrying standalone cyber insurance. In contrast, 33% of Baa-rated issuers report having coverage.

Higher-rated issuers, including states, are more likely to have the financial resources to invest in standalone insurance than lower-rated issuers. Furthermore, because of the increased frequency of attacks, the cost of insurance is increasing, making it harder for issuers with thin reserves to enter the market. Generally speaking, without insurance, entities may be challenged to navigate ransom negotiations, and incur greater costs in recovering and restoring data.

While standalone coverage is undoubtedly a strength for regional and local governments, governments also protect themselves in other ways. In many states, municipalities are insured through large risk pools, which protect entities from various liabilities, including cyberattacks. These pools are often less costly than purchasing a standalone plan. Alternatively, some local governments have either earmarked reserves to address cyber incidents or have ample general fund balance to cover a revenue interruption and/or cost of recovery. In Texas, for instance, a school district's debt service payment was diverted into a fraudulent account. The district had enough in excess fund balance to cover the payment without impairing its credit profile. Finally, if a cyberattack disrupts and delays a government's primary revenue stream, as experienced by a Louisiana school district in 2020, most entities have the ability to access the capital markets, and engage in short-term cash flow borrowing.

Lastly, governments take advantage of state and federal resources, such as law enforcement or Federal Emergency Management Agency (FEMA) dollars, to navigate an incident without suffering financially. In another incident in Louisiana in 2019, the state declared a state of emergency, and deployed law enforcement agents to affected school districts. If a local government is in a state that offers these resources, a lack of insurance does not necessarily mean the entity is unprotected.

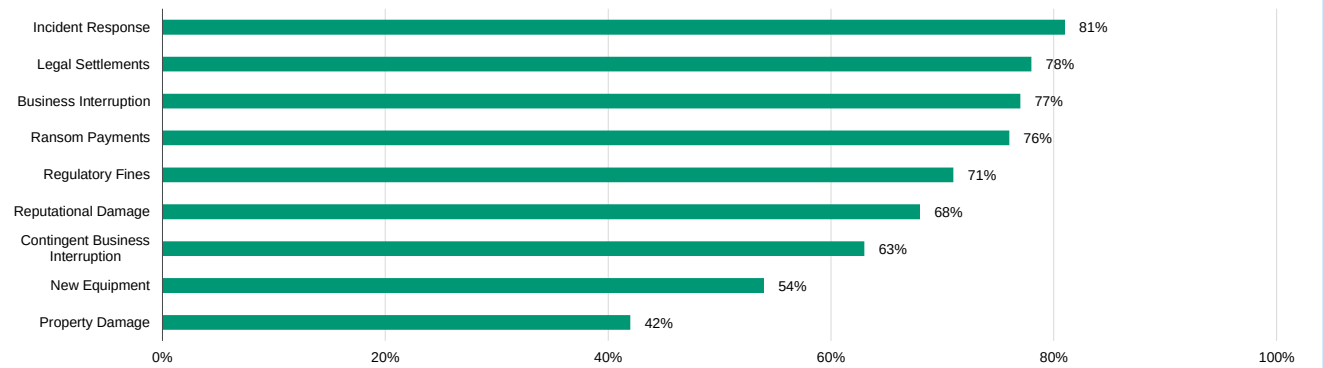
Most cyber policies cover incident response costs, but fewer cover property damage

If an issuer has a dedicated cyber policy, the specifics of what an insurer covers varies plan to plan (see Exhibit 12). Based on our survey results, most governments' policies include the cost of incident response, legal settlements, business interruptions and ransom payments. Less common is a plan that covers the purchase of new equipment and property damage. Although software and hardware replacement can be expensive, issuers have the option of using excess reserves or issuing debt, although, if done to a material degree, this could weaken credit quality.

Exhibit 12

Policies help offset losses across a range of coverages

% of respondents with specified coverages



Source: Moody's Investors Service

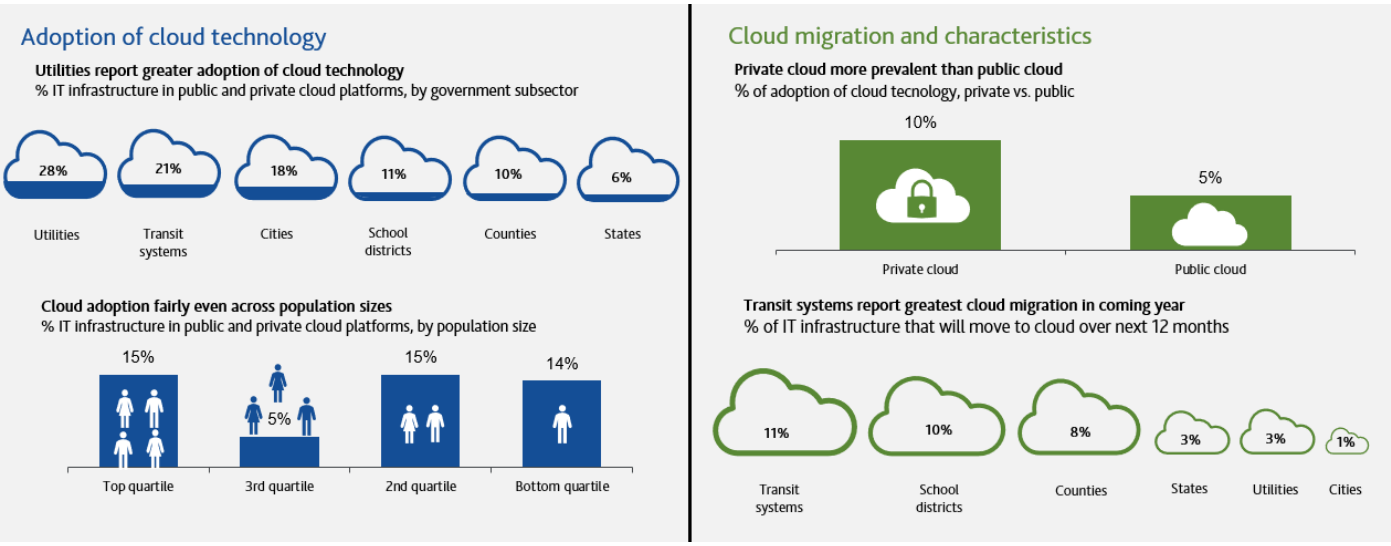
Adoption of cloud technology is relatively slow but is likely to grow

Regional and local governments have been slower than the private sector to adopt cloud technology. Cloud hosting, whether public or private, allows governments to outsource some of their cyber risk management to third-party providers, which typically offer greater security and can more readily make security updates to software and networks than in an on-premise IT environment.

Adoption of cloud technology was most prevalent among utilities and transits, as shown in Exhibit 13, with 28% and 21%, respectively, reporting their IT infrastructure is hosted on private or public cloud platforms. States, counties, and school districts are not nearly as aggressive.

Exhibit 13

All subsectors are increasing their reliance on cloud computing, with private cloud preferred over public



Source: Moody's Investors Service

Private cloud use is generally more prevalent among our respondents than public. For instance, while utilities store 18% of their data on private clouds servers, only 10% is housed on public cloud servers. This trend of favoring private over public holds true across all sectors. With a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to a single organization. The network can be physically located at an organization's on-site data center or hosted by a third-party service provider.

Most issuers surveyed said they plan to reduce the amount of data hosted on site in favor of public or private cloud services, as shown in Exhibit 14. The largest increases are likely among transit and utility systems, with transits planning to store 38% of their data on the cloud and utilities expecting 30% on the cloud in the next year. Counties and school districts plan to double their usage within the next 12 months.

Exhibit 14

Most sectors are increasing cloud usage in the next 12 months

	School districts	Cities	Counties	Utilities	Transit systems	States
% of IT infrastructure hosted on cloud in 2020	11%	18%	10%	28%	21%	6%
% of IT infrastructure to be hosted on cloud in 2021	20%	15%	20%	30%	38%	9%

	Aaa	Aa	A	Baa
% of IT infrastructure hosted on cloud in 2020	7%	15%	15%	18%
% of IT infrastructure to be hosted on cloud in 2021	10%	22%	26%	35%

	Top quartile	3rd quartile	2nd quartile	Bottom quartile
% of IT infrastructure hosted on cloud in 2020	15%	5%	15%	14%
% of IT infrastructure to be hosted on cloud in 2021	20%	7%	20%	17%

Source: Moody's Investors Service

Public and private clouds each have their advantages. With a public cloud, costs are generally lower, and there is less maintenance. With private, there is more flexibility, since an organization can customize the product, and more control and privacy. Based on our survey respondents, utilities and cities have chosen to make greater investment in private clouds, perhaps to take advantage of greater network security. However, cloud adoption in general indicates a forward-leaning and more sophisticated cyber program.

In contrast to the findings on cyber insurance, lower-rated issuers were more likely to use cloud technology than higher-rated peers, likely because it is less costly than housing data on-premise. For instance, in 2020, Baa-rated issuers reported 18% of data was on the

cloud compared with 7% by Aaa-rated issuers. By 2021, our lowest-rated entities plan to increase their investment to 35%, more than triple the Aaa-rated entities' 10%.

Moody's related publications

Sector reports

- Banks - North America: Cybersecurity strength rests on governance and prevention, March 2021
- Insurers, Insurance Brokers and Asset Managers — Global: Survey signals cybersecurity strength, with some differences across sectors, regions, March 2021
- Cyber Risk - Global: Sunburst attack on public and private entities raises credit risks as extent of breach unfolds, February 2021
- Cyber Risk - Global: 2021 Outlook – Cyber vulnerabilities in software supply chains, rising cost of ransomware will be key risks, January 2021
- Electric Utilities - Global: Cybersecurity readiness depends on scale, business model and generation ownership, November 2020
- Corporates – Global: Suppliers and vendors are becoming the weakest link in corporate cybersecurity, June 2020
- Cyber Risk – Global: Digitization and attack sophistication will pose heightened cyber risks in 2020, January 2020
- Local Government - US: Ransomware attacks highlight importance of IT investment and response planning, October 2019
- Cyber Risk – Global: Cyber disclosures reveal varying levels of transparency across high-risk sectors, October 2019

Sector comments

- Local Government - New Jersey: Joint insurance funds help smaller municipalities lower cyber, social risks, November 2020
- Local Government - Ohio: State's creation of Cyber Reserve will help mitigate risks from cyberattacks, November 2019
- State and Local Governments - Louisiana: State-coordinated response improves school districts' outcomes in cyberattacks, August 2019

Topic page

- Cyber Risk

Endnotes

1 We defined larger governments as serving a population greater than 766,000 with the largest having a population of over 3.2 million. Smaller governments are those with populations less than 766,000, with the smallest serving populations of less than 160,000. State and transit authorities are typically part of the former while many cities and school districts fall into the latter

2 https://oese.ed.gov/offices/education-stabilization-fund/elementary-secondary-school-emergency-relief-fund/

REPORT NUMBER 1268980

Contacts

Brian Barkman +1.212.553.6934
Associate Analyst
brian.barkman@moodys.com

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

MOODY'S
INVESTORS SERVICE