MOODY'S INVESTORS SERVICE

SECTOR IN-DEPTH
25 November 2019

Rate this Research

Contacts

David Rogovic +1.212.553.4196
VP-Senior Analyst
david.rogovic@moodys.com

William Foster +1.212.553.4741
VP-Sr Credit Officer
william.foster@moodys.com

Edward Demetry +44.20.7772.1720
Analyst
edward.demetry@moodys.com

Nina Delhomme +44.20.7772.1086
Associate Analyst
nina.delhomme@moodys.com

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

Leroy Terrelonge 1.212.553.2816
AVP-Cyber Risk Analyst
leroy.terrelonge@moodys.com

Lesley Ritter +1.212.553.1607
Vice President – Senior Analyst
lesley.ritter@moodys.com

Marie Diron +65.6398.8310
MD-Sovereign Risk
marie.diron@moodys.com

David Rubinoff +33.1.5330.3419
MD-Sub Sovereigns
david.rubinoff@moodys.com

Alastair Wilson +44.20.7772.1372
MD-Global Sovereign Risk
alastair.wilson@moodys.com

Jim Hempstead +1.212.553.4318
MD-Utilities
james.hempstead@moodys.com

Cyber Risk – Global

Cyberattacks on governments are rising but pose limited risks to credit quality

The growing interconnectedness of digital networks and the expanded use of technology to deliver government services have increased governments' exposure to cyberattacks, both through direct assaults on their own systems and through the impact of attacks on the broader economy. While governments worldwide are vulnerable to cyberattacks, the associated risks to their credit quality are limited. For bigger governments, including sovereigns and larger regional and local governments (RLGs), the scale and diversification of their economies and sizable financial buffers enhance their ability to withstand cyberattacks. Smaller RLGs typically have fewer protections because of their smaller economies and more limited financial resources.

» **Digital technologies and e-services have increased the cyberattack exposure of governments.** Sovereigns are more vulnerable than RLGs to attacks that target highly sensitive data, such as confidential national security information, or that disrupt critical infrastructure or services. More sophisticated cyber actors, including state-sponsored groups with geopolitical interests, typically target sovereigns and are often driven by espionage or the intent to disrupt domestic politics, including through election interference. In contrast, RLGs typically are targets of financial opportunity, because their legacy information technology (IT) systems can be vulnerable to ransomware. Socially motivated actors, such as hacktivists, target both sovereigns and RLGs.

» **Cyber risks vary for governments, but large diversified economies and ample fiscal resources help insulate them to varying degrees.** These qualities highlight the generally lower impact of a cyberattack against governments than against private companies. In addition, unlike businesses, governments do not face the same risks of losing customers or damage to their brands in the aftermath of an attack. For sovereigns, the credit implications of an attack would most likely result from a weakening of institutions and governance strength or from heightened political risk. For RLGs, the main impact would likely be on economic fundamentals and financial performance.

» **Cyber defense capabilities are often reflected in the strength of government institutions.** Although a well-developed cybersecurity strategy does not necessarily reduce a government's vulnerability to attack, it can reduce an attack's severity. Strong cyber defense capabilities can inform how quickly a government can respond to a cyber event, which will help limit the credit impact. These capabilities include ample cybersecurity resources, and cyber-specific incident and crisis management teams. In general, more advanced economies with stronger institutions tend to have the most developed cybersecurity strategies and defense capabilities.

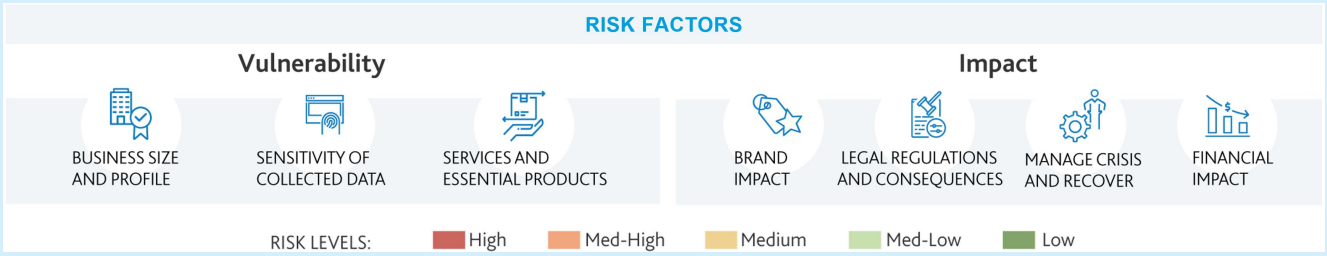
Moody's approach to assessing cyber risk

This report builds on our previous research on cyber risk across sectors to explain in more detail how we incorporate cyber risk into our credit analysis of governments. Our assessment focuses on how a cyberattack would affect the factors in our rating methodologies for sovereigns and RLGs, which drive the ultimate credit impact.

Our framework for assessing cyber risk for governments follows our approach to assessing cyber risk across all sectors globally, which takes into account the risk factors in each sector. An individual entity's cyber risk exposure is in large part defined by the risks of the sector, as well as by the entity's own business processes and activities. In developing our framework for analyzing relative levels of cyber risk, we consider the typical debt issuer in each sector along two dimensions. The first dimension is **vulnerability** to the type of attack or event to which the entities in a given sector are exposed. The second dimension is **impact**, including the disruption of critical business processes, loss of data access or heightened reputational risk, each of which can lead to financial stress, such as increased expenses for recovery or reductions in revenue, or lower institutions and governance strength and increased political risks in the case of governments (see Exhibit 1).

Exhibit 1

Cross-sector assessment of cyber risk focuses on vulnerability and impact



Source: Moody's Investors Service

Under our framework, our credit assessment of cyber risk reflects our assessment of the vulnerability to an attack and the severity of impact on an entity's creditworthiness. Given the evolving nature of cyberattacks, we do not assign a probability to the likelihood of attack, but we assess the credit impact of a successful cyberattack. Through this framework, we assess cyber risk for governments overall as medium-low, which combines our assessments of medium vulnerability to a cyberattack with low financial and reputational impact of an attack (see Exhibit 2).

Exhibit 2

Cyber risk assessment for sovereigns and RLGs

Sovereign			
OVERALL Medium-Low	VULNERABILITY: Medium IMPACT: Low	$35,778.5 billion	Rated debt
Regional & Local Governments			
OVERALL Medium-Low	VULNERABILITY: Medium IMPACT: Low	$3,008.4 billion	Rated debt

Data on outstanding debt includes Moody's-rated debt only and is as of August 2018. For rated sovereigns, debt outstanding totals $60.5 trillion when including both rated and unrated debt.
Source: Moody's Investors Service

Digital technologies and e-services have increased the cyberattack exposure of governments

Governments are susceptible to cyberattack for a variety of reasons and are vulnerable to attack from multiple types of actors. This vulnerability has increased in recent years, consistent with the rise of digitization, the growing interconnectedness of digital networks and the increased use of technology to store personal information and deliver services to residents (e-services), such as government transfers and the ability to make tax payments online.

Larger government entities, including both sovereigns and bigger RLGs, tend to have high public profiles, substantial resources and revenue bases, and control over confidential information. As a result, these entities are attractive targets for cybercriminals. A sovereign government's central role in payment and clearing systems, typically through its central bank, also increases vulnerability. Meanwhile, all governments, regardless of size, possess sensitive data to some degree and provide essential services.

The risk factors vary for different governments, as do the types of perpetrators who target them. Sovereigns tend to be vulnerable to attacks that seek access to sensitive or confidential data, such as national security information, often driven by espionage, or that disrupt critical infrastructure or government services. Cyberattacks on sovereigns also generally require a high level of sophistication; the perpetrators will likely be well-organized cybercrime groups or state-sponsored actors with geopolitical interests. For example, the US Department of Homeland Security lists cyberattacks by national governments, for cyberwarfare purposes, and by foreign intelligence services, for information-gathering and espionage activities, to be a major source of cyber threats to the US (Aaa stable). According to the department, the only entities developing capabilities that could cause widespread, long-lasting damage to US critical infrastructure are nation states.[1]

In contrast, RLGs are generally more vulnerable than sovereigns to financially motivated, opportunistic cyberattacks, particularly those that use ransomware.[2] In these types of attacks, cybercriminals seek to block access to an organization's critical data or systems unless they receive payment. The number of ransomware attacks has increased significantly over the past two years, particularly in the US (see box on page 6 for details).

Less-sophisticated perpetrators, such as individual hacktivists and smaller-scale cybercrime groups, can carry out successful attacks on RLGs. These types of attacks are more common for smaller RLGs, which are susceptible to cyber breaches as a result of legacy IT systems that have not been adequately updated and have fewer security controls. Hackers may also target a local government for sociopolitical reasons. For instance, cyberattackers in 2016 hit North Carolina's government website in protest of a controversial state law.

Cyberattacks can take many forms with varying degrees of impact on government systems and information. In the information security community, the confidentiality, integrity and availability (CIA) triad framework provides one approach to defining threats and vulnerabilities based on the potential impact of a cyberattack on government information and critical systems (see Exhibit 3). In this context, each category is defined as follows:

» *Confidentiality:* attacks that give access to unauthorized users such as through espionage, data breaches, theft of intellectual property, and leaks

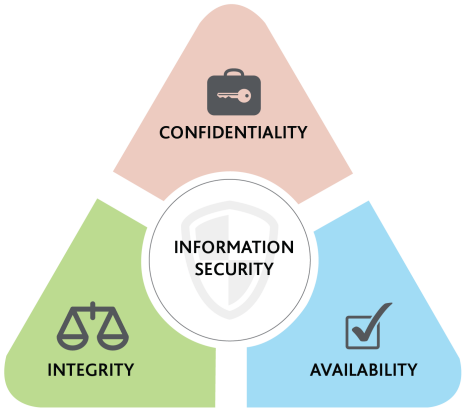
» *Integrity*: attacks in which data has been tampered with, for example by manipulating election results, changing payment details, and corrupting sensitive data

» *Availability*: attacks in which information can no longer be accessed, including destructive attacks such as WannaCry and NotPetya, ransomware attacks, and distributed denial-of-service (DDoS) attacks

Exhibit 4 demonstrates how this framework can be applied to define the impact that various cyberattacks have had on sovereign and RLG governments worldwide.

Exhibit 3

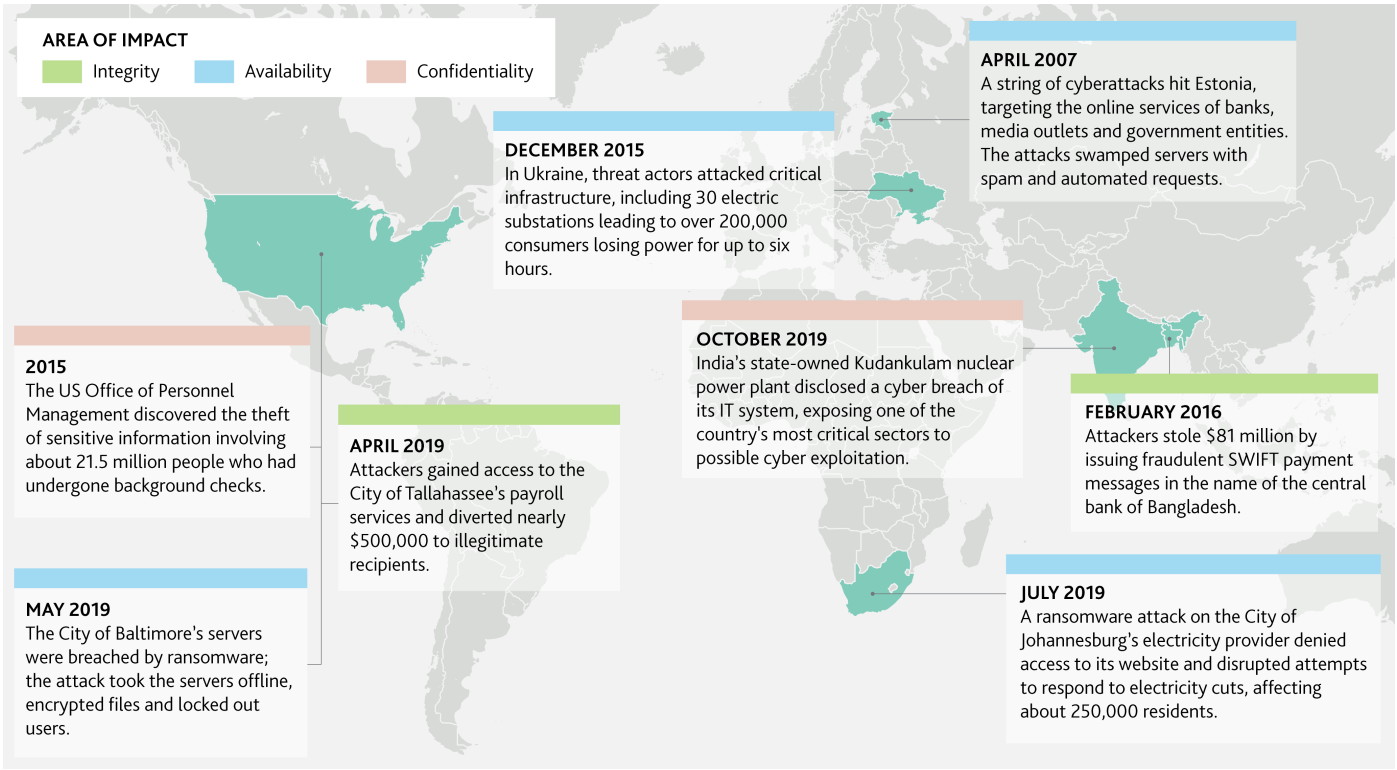
The CIA triad framework evaluates potential impact of a cyberattack in three key areas …



Source: Moody's Investors Service

Exhibit 4

… which can be applied to a range of cyberattacks worldwide



Source: Moody's Investors Service

Cyber risks vary for governments, but large diversified economies and ample fiscal resources help insulate them to varying degrees

Governments are attractive targets for cyberattackers as a result of their large financial resources, the essentiality of the services they provide and the sensitivity of the data they collect. However, they are broadly resilient to cyberattacks from a credit quality perspective. Unlike private companies, governments oversee large and diverse economies, which helps distribute associated risks. Governments typically also have ample fiscal resources and taxing authority to absorb the potential financial costs of a successful cyberattack. Additionally, governments do not face the same types of reputational or regulatory risks as do private businesses following

cyberattacks. For companies, reputational costs, potential loss of customers and litigation expenses can have significant effects on their financial operations. In contrast, such risks are largely absent for governments.

We assess the credit implications of a cyberattack on governments through the impact on the factors in our respective rating methodologies for sovereigns and RLGs (see Exhibit 5). For sovereigns, we examine the impact on factor scores that assess economic, institutional and fiscal strength, as well as susceptibility to event risk, primarily through political risk. For RLGs, we examine the impact on their Baseline Credit Assessments through idiosyncratic risk scores for economic fundamentals, governance and management, financial performance and debt. We also factor in systemic risk, which applies to all RLGs in a country and is driven by the respective sovereign's risk.

Exhibit 5

Channels through which a hypothetical cyber event could weaken government credit profiles

Ratings Methodology Factor Scores				
Sovereign	*Regional & Local Governments (RLGs)*		Hypothetical cyber event	Credit impact
Economic strength	*Economic fundamentals*		An attack on critical infrastructure could disrupt economic activity, or an attack could be perpetrated on a smaller, less diverse government that relies on a single industry as a source of growth.	Economic growth could slow significantly and economic strength could be impaired.
Institutions & governance strength	*Governance & management*		A cyberattack could expose sensitive information that reveals institutional arrangements that are weaker than previously thought.	Our assessment of institutional effectiveness and quality of governance could decline materially.
Fiscal strength	*Financial performance & debt portfolio*		While rare, fiscal costs associated with a cyberattack could be so large that they result in weaker overall fiscal strength for sovereigns, or weaker financial performance and debt profiles for RLGs.	Financial resources and fiscal strength could decline.
Susceptibility to event risk (Political risk)	*NA*		A cyberattack could attempt to disrupt domestic or geopolitics, including through direct or indirect election interference.	Political risk could rise.

Source: Moody's Investors Service

In general, disruption of government services, including critical infrastructure, presents a greater risk to economic activity than does loss of data. Therefore, services disruption represents a greater threat to our assessment of a government's economic strength and fundamentals. For sovereigns and large RLGs, economic resilience and fiscal resources will limit the direct credit implications of an attack that only temporarily disrupts economic activity. The credit implications are more likely to be revealed through consequences for institutions and governance strength or political risk, including through our assessment of how quickly and effectively the sovereign or RLG responds to the attack. For smaller RLGs, particularly those with more limited financial resources, the primary channel through which a cyberattack could weaken credit quality is through disruption of economic activity and the associated financial costs, which could contribute to a higher debt burden.

Large size, diversity and dynamism of economies mitigates economic impact of most cyberattacks

The size, dynamism and diversity of the economies of sovereigns and larger RLGs contribute to economic resilience that will mitigate the potential credit impact of most cyberattacks. Business diversification is an important consideration in assessing cyber risk, and governments generate revenue from multiple streams (corporate and individual taxpayers) and in multiple forms (income tax, value-added tax, import duties and excise taxes). These considerations highlight the economic diversification of RLGs and sovereigns compared with business diversification at the corporate level.

The economic impact for governments would likely be the most severe in the event of an attack that targets critical infrastructure and paralyzes a large proportion of the economy or many large companies operating in a country or city. In this context, the size of a government and its related entities is relevant, resulting in higher risks for smaller RLGs who are less likely to be able to rely on robust backup infrastructure.

High-profile examples of cyberattacks on sovereigns and RLGs

In June 2015, the US Office of Personnel Management (OPM) revealed that it had been the target of a massive data breach, one of the largest ever breaches of US government data. The breach involved the theft of about 21.5 million records of classified, personally identifiable information on government and some nongovernment employees who had undergone background checks.[3] An investigation concluded that Chinese state actors were likely responsible for the breach. Earlier in 2015, OPM discovered that the personnel data of 4.2 million current and former federal government employees had been stolen. Although the episodes involved highly sensitive government information, they did not weaken the creditworthiness of the US sovereign.

Similarly, cyberattacks in Estonia (A1 stable) in 2007 and more recent attacks in Ukraine (Caa1 stable) have had no material impact on the creditworthiness of those sovereigns. The Estonia attacks affected government websites, banks and newspapers, disrupting activity for about a month. In Ukraine, cyberattackers hit critical infrastructure, including an attack on regional electricity distribution company Kyivoblenergo in 2015. That attack resulted in 200,000 consumers losing power for several hours. The relatively short duration of the outage demonstrated the government's capacity to recover from an attack. In addition, Saudi Arabia's state-owned oil company, Saudi Aramco (A1 stable) was attacked by malware in 2012 and 2017.

For RLGs, the number of ransomware events has jumped over the past two years, particularly in the US. These events have included attacks on larger US cities such as Baltimore (Aa2 stable) and Atlanta (Aa1 stable), as well as attacks on smaller cities in Florida, Alaska and Texas. The City of Johannesburg, South Africa, was also subject to a recent attack that targeted its electricity provider, City Power.

From a credit standpoint, large cities have been able to withstand ransomware attacks even as the costs have totaled in the millions of dollars. Both Baltimore and Atlanta, for example, are regional economic hubs with a substantial institutional presence. Their large budgets and access to sufficient liquidity to cover accelerated short-term costs helped limit any potential impact of the attacks on their creditworthiness. The May 2019 attack on Baltimore hobbled city operations for nearly two months, resulting in short-term costs of about $18 million. However, the costs to restore its systems represented less than 1% of the city's revenue and 2.4% of its liquidity. The March 2018 ransomware attack on Atlanta was more significant, but manageable. The attack's preliminary costs totaled $10 million to $15 million, equivalent to about 2% of the city's revenues and around 7.2% of cash reserves. All of Atlanta's associated costs were fully reimbursed by cyber security insurance.

Government fiscal resources mitigate financial impact of most cyberattacks

The cost of a typical cyberattack tends to be small compared with the large resources that most sovereigns and RLGs possess. According to the Ponemon Institute, a data protection research firm, the global average cost of a data breach was just under $4 million in 2019, a small amount overall for most government entities.

An attack on critical infrastructure, which results in a broad economic slowdown, would weaken fiscal accounts through reduced tax revenue and increased spending on repairs. To the extent that these effects materially increase a government's debt burden, a cyberattack could result in a change in our assessment of a sovereign's fiscal strength, or in our assessment of the financial performance or debt profile of an RLG.

In most cases, however, the financial cost of a cyberattack is likely to be small compared with the size of the government's balance sheet and financial resources. For instance, the attack on the central bank of Bangladesh (Ba3 stable), which resulted in a loss of more than $80 million, did not alter our assessment of the sovereign's fiscal strength, given the very small size of the costs relative to the overall economy (about 0.027% of nominal GDP) and the resources available to the government. In another example, Saudi Arabia's state-owned oil company, Saudi Aramco (A1 stable), which contributes to the government budget via royalties, taxes and dividends, has been hit by numerous cyberattacks in the past few years.[4] However, the attacks have not weakened the government's public finances, a result of Aramco's size – it is the world's largest oil producer – and healthy financial performance.

Most RLGs on the other hand have fewer resources than do sovereigns and are therefore more vulnerable to cyberattacks, particularly financially motivated ransomware attacks. Such attacks would need to be very large relative to an RLG's resource base to weaken operating performance or debt levels. Our assessment of the impact of a cyberattack on an RLG's financial performance and debt would also incorporate a given entity's access to liquidity and how quickly it could tap financial markets if required. Although

ransomware attacks have cost some cities, including Baltimore and Atlanta, substantial amounts, none of the reported attacks have significantly weakened their financial performance or debt levels, due to ample budgets and access to sufficient liquidity to cover accelerated short-term costs.

Preparedness for cyberattack and effectiveness of response will reveal governments' degree of institutional capacity

To date, cyberattacks have not materially influenced our assessment of institutions and governance strength of any sovereign or the governance and management of any RLG. However, cyberattacks could expose sensitive information that reveals weaknesses in institutional arrangements. For instance, the Panama Papers leak in 2016 exposed information that resulted in political fallout for government officials in countries including Iceland (A3 positive), Pakistan (B3 negative), Malta (A2 stable), Spain (Baa1 stable) and Mongolia (B3 stable). Another example is the more recent cyber breach of India's (Baa2 negative) largest operating nuclear generation facility, the state-owned Kudankulam nuclear power plant. The event exposed one of the country's most critical sectors to possible cyber exploitation that could result in operational degradation or disruption, or intellectual property theft.[5]

Governments' responses to shocks often reveal institutions and governance strength. For sovereigns and RLGs, capacity to respond promptly and effectively to a cyberattack would be a key factor in assessing any impact on the government's creditworthiness. A cyberattack could reveal information pointing to unexpected weaknesses in the institutional framework that contributes to a weaker overall assessment of institutions and governance strength.

For RLGs, we would assess the impact of a cyberattack on governance and management in terms of preparedness and capacity to respond. A strong active management response to a cyberattack can mitigate the damages and ultimate credit impact. For example, the response by the Colorado Department of Transportation to a ransomware episode in 2018 highlights how institutional policies and responsiveness can mitigate the impact of an attack. The state had defenses that allowed it to react quickly and limit the financial cost of the attack to only $2 million.

Political risk captures risk of cyberattack for some sovereigns

For some governments, cyber risk is captured in our assessment of political risks. This is likely to be the case when a government is vulnerable to more frequent attacks from state-sponsored organizations. A government's elevated vulnerability to cyber risk will be driven by exposure to potential cyber warfare resulting from heightened political conflict, or from hostile relations with another government that has strong cyber capabilities and the motivation to carry out an attack. For instance, state-sponsored groups have reportedly carried out cyberattacks against Estonia and Ukraine. However, this risk is only one dimension of the many facets that contribute to a country's final political risk assessment. Where relevant, our final political risk score would capture a cyberattack by a state-sponsored actor that targets another government.

Thus far, cyberattacks that seek to disrupt domestic politics or influence election outcomes have ultimately had no direct credit implications. Politically motivated cyberattacks can take the form of targeted attacks on election commissions or on a political party, with the aim of spreading disinformation, influencing behaviour or making a particular website unavailable. A recent study by the University of Oxford on global disinformation and social media manipulation states that a handful of state actors regularly use computational propaganda for foreign influence operations.[6] In particular, Facebook and Twitter, two of the world's largest social media platforms, have attributed foreign influence operations to China (A1 stable), India, Iran, Pakistan (B3 negative), Russia (Baa3 stable), Saudi Arabia and Venezuela (C stable). The study found evidence of formally organized cyber propaganda campaigns in 56 countries through Facebook, which remains the platform of choice for social media disinformation. Some of this activity specifically targeted elections.

Although there have been many reported cases of cyberattacks related to elections, including in the US, France (Aa2 positive), Germany (Aaa stable), Hong Kong (Aa2 negative), Israel (A1 positive) and throughout the Commonwealth of Independent States (CIS), these episodes have not had an impact on a government's creditworthiness. Thus far, despite multiple reported cases, it has been very difficult to prove with absolute certainty that a cyberattack occurred and resulted in material election interference. Meanwhile, clearly determining the ultimate impact on final election results is highly challenging. Nonetheless, if there were a successful cyberattack that was indeed proven with certainty and that resulted in clear interference with final election results, it could have credit implications. Especially if the outcome were to lead to a clear shift toward more credit-negative policy developments.

Cyber defense capabilities are often reflected in the strength of government institutions

Although a well-developed cybersecurity strategy does not necessarily reduce a government's vulnerability to attack, it could reduce an attack's severity and therefore limit the negative credit implications. Strong cyber defense capabilities can inform how quickly a government reacts to a cyber event, which can influence the overall credit impact. These capabilities vary widely across the sovereign and RLG universe, but tend to be higher in more advanced economies with stronger institutional frameworks.

In response to growing threats, governments have developed defense capabilities and strategies to lessen their vulnerability to cyberattacks and the impact of successful attacks. Well-developed cyber strategies, which include cyber-specific incident and crisis management teams, especially when combined with the necessary technical skills, can increase responsiveness to an attack and limit its duration or severity. For example, Estonia, a leader in providing digitized government services to its citizens, invests heavily in its Defense League Cyber Unit to protect against the risks associated with increased use of e-services. Similarly, in the Netherlands (Aaa stable), the 2018 Dutch Cyber Security Agenda has committed to allocate 95 million euros annually for structural funding of cybersecurity. In the US, President Trump's fiscal year 2019 budget authorized $15 billion for cybersecurity-related activities.

Governments have also used regulations to strengthen cybersecurity. For example, in 2016 the European Union (Aaa stable, EU) established cybersecurity rules for firms supplying services deemed essential (including energy, transport, finance or health). Also in 2016, China implemented a national cybersecurity law to force specific sectors to invest in reducing cybersecurity risks.

A starting point for assessing defense capabilities is to examine whether a government has a cybersecurity strategy that focuses on cyberattack prevention, detection and response. The National Cyber Security Index identifies 126 countries globally that have either a cybersecurity strategy or a cyber incident response unit in place.

If a cyberattack occurs, we will assess the steps taken to implement this strategy across different levels of government. In general, more advanced economies with stronger institutional frameworks, such as the US or countries in the EU, tend to have the most developed cybersecurity strategies and defense capabilities. In a few cases, smaller countries like Estonia and Israel are leaders in cybersecurity through continued investment in their capabilities.

Government cyber risk strategies usually apply a top-down approach and therefore policies at the sub-sovereign level tend to rely on strategies adopted by, and sometimes resources provided by, the federal government. However, broader resource constraints can pose challenges. For example, RLGs, much more than sovereigns, often lack staff with cybersecurity expertise, in part because of lower salaries compared with those at the federal government level or in the private sector. Additionally, RLG budgets generally focus on social service provision, resulting in relatively unbalanced spending priorities. This can contribute to lower visibility and control of cybersecurity risks, due to more limited investment in cybersecurity infrastructure, use of outdated and aging legacy systems, lower IT expertise and lack of a clearly defined cybersecurity strategy.

Thus far, neither our assessment of a government's cybersecurity strategy, nor its response to a cyberattack, has led to a change in our overall assessment of a sovereign's institutions and governance strength or an RLG's governance and management. This is in part due to the broad range of variables that are considered when assessing a government's institutional and governance framework[7], which ultimately limits the impact of any one particular variable.

Moody's related publications

Issuer research

» City of Johannesburg (South Africa): Response policy mitigates impact of cyberattack, July 2019

» Baltimore (City of) MD Second ransomware attack in 15 months disrupts Baltimore's operations, May 2019

» Matanuska-Susitna (Borough of) AK: Quick, coordinated response, access to emergency funds and insurance limit cyberattack losses, March 2019

Sector research

» Regulated utilities and power companies - North America: Grid modernization heightens vulnerability of utilities to cyberattacks, November 2019

» Infrastructure & Project Finance – Global: Cyberattack on Indian nuclear plant shows vulnerabilities of critical infrastructure, November 2019

» Sovereigns - Global: Digital technologies likely to enhance credit profiles for countries that leverage benefits while managing disruptions, November 2019

» Cyber Risk – Global Investment Banks: GIBs heighten readiness against constant cyber threat, October 2019

» 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

» Hospitals & health service providers - US: Cyberattacks pose growing operational and financial risks for hospitals, September 2019

» Corporates - Global: Deepfake disinformation campaigns pose reputational risks to businesses, August 2019

» State and local government – Louisiana: State-coordinated response improves school districts' outcomes in cyberattacks, August 2019

» Sovereigns – Global: Artificial intelligence credit positive for sovereigns, effects will take time to emerge, June 2019

» Cross-Sector - Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019

» Local government – Washington: Washington State cybersecurity audits help mitigate risk from growing threat, August 2018

» Public power electric utilities - US: Growing grid interconnectivity increases cybersecurity risks, June 2017

Topic page

» Cyber Risk

» Technology and Innovation

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.

Endnotes

1 US Department of Homeland Security's Cyber Threat Source Descriptions.

2 Local government - US: Ransomware attacks highlight importance of IT investment and response planning, September 2019.

3 The breach included Social Security numbers, names, places and dates of birth, and addresses.

4 Saudi Arabia's oil sector, which is in effect represented by Aramco, contributed 83% of government revenue on average each year over the 1995-2014 period. This proportion fell to 67% on average over the 2015-18 period but remains significant. See Credit Opinion, Saudi Arabian Oil Company, April 1, 2019.

5 See: Infrastructure & Project Finance – Global: Cyberattack on Indian nuclear plant shows vulnerabilities of critical infrastructure, November 2019

6 Samantha Bradshaw & Philip N. Howard. (2019) The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation, Working Paper 2019.2. Oxford, UK: Project on Computational Propaganda.

7 For sovereigns, these include quality of legislative and executive institutions, strength of civil society and the judiciary, and fiscal and monetary policy effectiveness; for RLGs these include risk controls and financial management, investment and debt management, and transparency and disclosure.

REPORT NUMBER 1172789

MOODY'S
INVESTORS SERVICE