

## SECTOR IN-DEPTH

26 February 2019



Rate this Research

### TABLE OF CONTENTS

Cyber risk continues to rise	2
Assessing sector exposure to cyber risk: Our approach	3
Sector-level risk assessments	6
Appendix I: Summary of high-risk sectors	15
Appendix II: Summary of medium-high risk sectors	17
Appendix III: Summary of medium-risk sectors	21
Appendix IV: Summary of medium-low risk sectors	25
Appendix V: Summary of low-risk sectors	28
Moody's related publications	30

### Contacts

Derek Vadala +1.212.553.4787  
MD-Global Cyber Risk  
derek.vadala@moodys.com

Robard Williams +1.212.553.0592  
Senior Vice President/CSR  
robard.williams@moodys.com

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

Alessandro Roccati +44.20.7772.1603  
Senior Vice President  
alessandro.rocatti@moodys.com

Stephen Sohn +1.212.553.2965  
Senior Vice President  
stephen.sohn@moodys.com

Vincent Gusdorf, CFA +33.1.5330.1056  
VP-Senior Analyst  
vincent.gusdorf@moodys.com

Kurt Krummenacker +1.212.553.7207  
Senior Vice President/Manager  
kurt.krummenacker@moodys.com

## Cross-Sector - Global

# Credit implications of cyber risk will hinge on business disruptions, reputational effects

The growing intersection of supply chains, connectivity and access to data is increasing the potential for significant cyber attacks, creating new risks for governments and businesses worldwide. In this report, we assess the inherent cyber risk exposure of 35 broad sectors based on two factors: vulnerability to a cyber event or attack, and impact in terms of potential disruption of critical business processes, data disclosure and reputational effects. Highlights of our analysis include:

- » **Four sectors with \$11.7 trillion in rated debt outstanding are at high risk.** These sectors are banks, securities firms, market infrastructure providers and hospitals, all of which rely heavily on technology for operations, content distribution or customer engagement. Of the remaining 31 sectors that we evaluated, nine are at medium-high risk and include electric utilities, health insurance, retail, manufacturing and autos, telecommunications and media, and technology. These sectors rely on data and technology but have characteristics that can limit the impact of cyber events, such as customer stickiness or the ability to control pricing. Sectors at the lower end of our scale offset impact through the ability to use manual processes in case of business disruption, less reliance on interconnected technology and limited competition.
- » **Our assessments consider the overall financial impact of a significant cyberattack that could lead to a weakened credit profile.** We consider the likelihood and potential impact of cyberattacks at the sector level without taking into account existing cyber defenses of individual issuers, such as firewalls, monitoring capabilities and system backups. However, we consider mitigants that apply uniformly across an entire sector, such as monopolies or supply chain diversity. Financial impact could include cost of insurance, effect on customer behavior, litigation costs, fines and impact on technology infrastructure and R&D spending. Therefore, robust sources of liquidity remain a key mitigant.
- » **In our view, cyber risk is event risk and we see a rising tide.** Digitization continues to increase, supply chains are becoming more complex and attacker sophistication is improving. However, the universe of cyber threat actors remains the same: socially motivated attackers (hacktivists), criminals and nation states.
- » **We will continue to develop more frameworks related to individual issuers' cyber risk.** As cyber risk evolves, we will continue to engage in a dialogue with issuers on the topic, focusing first on higher-risk sectors as we develop assessment frameworks for individual issuers.

## Cyber risk continues to rise

The growing interconnectedness of both public and private sector entities has resulted in a significant increase in cyber risk. Since our prior publication examining sectorwide cyber risk (See [Cyber Risk of Growing Importance to Credit Analysis](#), November 23, 2015), we have further developed our views with regard to this issue. These new considerations include:

- » **Cyber events can have distinct global impact.** We continue to view cyber risk as event risk. A single event can have a swift and severe short-term impact on sectors and individual issuers, affecting supply chains, logistics, and productive capacity, and can also generate tail risk. However, cyber events have the potential for far-reaching effects, differentiating these events from more localized incidents such as severe weather events. For example, the 2017 NotPetya ransomware attack had impact far beyond its intended target, illustrating the disruptive potential of the most severe cyberattacks.<sup>1</sup>
- » **Disruption events are more significant than data disclosure.** We consider two basic outcomes of a cyber attack: business disruption and data disclosure. While companies and governments face potential cyber events that are specific to their individual business or organizational profiles, a prolonged disruption event is likely to eclipse even a significant data disclosure event across all sectors. The potential impact of an event that disrupts key business activities would not only affect an individual issuer directly, but it could also spread to entities in other sectors. For example, disruption of the electricity supply or of financial market infrastructure for an extended period would have far-reaching implications across many sectors. We view typical data disclosure events as unlikely to have the same impact as disruptions, although the largest of these disclosures have had damaging effects on individual companies, their management teams and shareholders, as was the case with cyber incidents at [Equifax Inc.](#) (Baa1 stable), [Target](#) (A2 stable) and Sony Pictures, a unit of [Sony Corporation](#) (Baa2 stable). In the case of Sony Pictures it was ultimately the disclosure of internal emails that led to the CEO's departure.
- » **Duration of a cyber event is a key factor.** When considering a disruption event, duration is critical in determining the direct financial effects and, in turn, the overall potential impact, especially for individual issuers. However, even an event with short duration can have a long-lasting impact — for example, an incident that is timed to coincide with a key market or revenue event. In addition, a short-term disruption of a critical provider (for example, a public cloud or electricity provider) can cause significant impact.
- » **Hacker capabilities have grown and collateral impact has risen.** The universe of threat actors has remained largely the same, encompassing individual hackers, organized hacktivists, criminals (including insiders), and nation states. But these groups now have greater capabilities as a result of the increasing sophistication and availability of tools and techniques following high-profile leaks of nation-state cyber weapons. As a result, global cyber events can now disrupt unintended targets, further underscoring the need for firms to secure technology and improve cyber resilience.
- » **New technologies and a lack of skilled cybersecurity workers contribute to risks.** In response to rising attacker capabilities, organizations worldwide need to continually raise their baseline security to avoid becoming unintentional collateral damage of attacks and easy targets of less-sophisticated hackers. The growing adoption and complexity of new technologies also contribute to the increased risks. Innovations such as cloud services are expanding in tandem with a talent gap for security and technology professionals who can implement and manage these services, as well as defend organizations.
- » **Attacks are still underreported.** Most reporting frameworks or regulations are still underdeveloped and focused on the breach of confidential personal data. As a result, public disclosure of cyber events often fails to include high-quality information about disruption events that do not rise to levels resulting in media scrutiny. These events may be attributed to technology or process failures rather than cyberattacks, or affect data not required to be reported under current rules. Therefore, public cyber disclosure is inconsistent and materiality is difficult to measure, and it remains an emerging practice without global standards or requirements. Furthermore, we may not always know if an issuer has been breached.

This publication does not announce a credit rating action. For any credit ratings referenced in this publication, please see the ratings tab on the issuer/entity page on [www.moody's.com](http://www.moody's.com) for the most updated credit rating action information and rating history.

- » **Our approach to quantifying the credit implications of cyber risk exposure is still evolving at the issuer level.** As cyber risk evolves, key factors in our credit analysis could include the extent of an entity's investment in cyber defenses before an event, post-event expenses related to incident response and recovery, customer (or taxpayer) compensation, regulatory fines, litigation, increased R&D spending to recover competitive advantage, and in some cases, longer-term impact as a result of reputational issues. The extent to which a given sector or entity has exposure to reputational risk associated with a cyber event and its sensitivity to prolonged disruptions will vary based on sector, size of the entity, geographic reach and relevant regulation.

### Assessing sector exposure to cyber risk: Our approach

The inherent cyber risk exposure of public and private entities is in large part defined by the sectors in which they operate and their business processes and activities. Accordingly, in developing our framework for understanding relative levels of cyber risk across sectors, we consider the median issuer in each sector along two dimensions: **vulnerability** to the type of attack or event to which entities in a given sector are exposed, and **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 political risks in the case of governments.

This approach provides a view of inherent cyber risk that only considers mitigation that would uniformly benefit the sector as a whole or generally benefit individual issuers equally during an event. Mitigants include having an effective monopoly, supply chain diversity, ability to fall back on manual processes, independent and localized operations, customer stickiness and pricing power. Given this approach, our sector analysis does not currently consider cybersecurity defenses such as insurance, firewalls, or system backups that individual issuers might employ.

When evaluating vulnerability, we generally consider the following characteristics – typical issuer size (based on revenue) and public profile, sensitivity of collected data, and essentiality of services provided relative to digitization – on a high-medium-low scale.

With regard to impact, we also use a high-medium-low scale in considering two primary types of cyber event risk, **data disclosure** and **business disruption**. We focus on whether the outcome of these events could materially weaken an issuer's financial profile or increase political and reputational risks. The financial impact could materialize in the form of short-term direct expenses (recovery costs, regulatory fines, incident response and legal fees) and in longer-term impact on financial results. These effects could include declining revenue as a result of customer turnover, the inability to attract new customers, or long-term regulatory consequences that increase operational expenses or even limit business growth. Prolonged impact on revenue and expenses could ultimately hurt an issuer's credit quality.

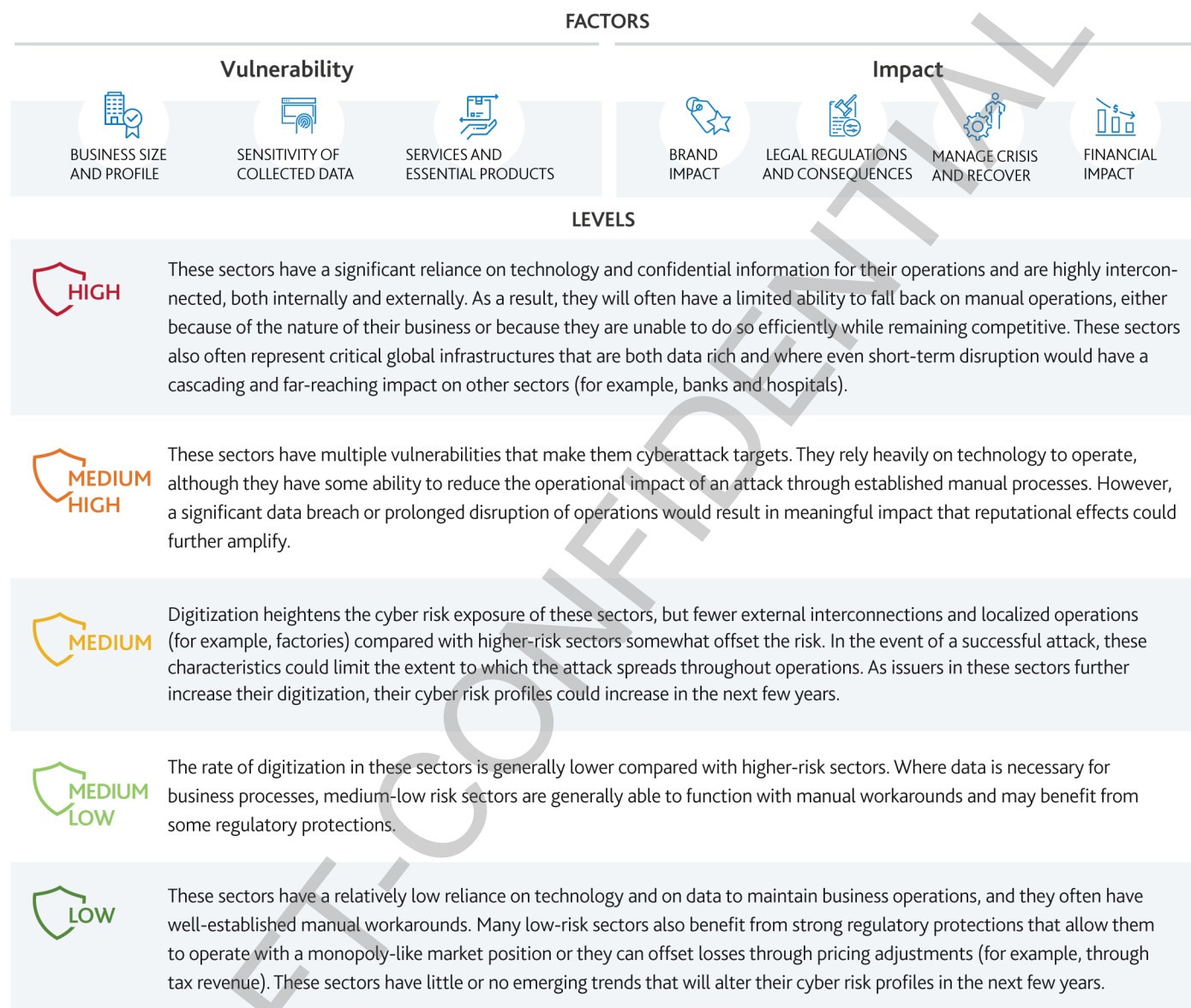
Data disclosure events encompass both the intentional and unintentional disclosure of confidential information. This data may include personal information that an organization or government collects on its customers or citizens, as well as intellectual property. Although in the past cyber criminals or malicious insiders were often the perpetrators of data breaches and disclosure, an increasing number of entities now face unintentional disclosure of confidential information as a result of improperly configured technologies such as the public cloud, or other breakdowns of internal controls.

Business disruption events include the interruption of key business processes and services as a result of attacks on underlying technology infrastructure. The extent to which an organization has compartmentalized its operations, and by extension its technology systems, can help limit impact.

The evaluation of a sector's vulnerability and the potential impact of a cyber event combine into an overall assessment on a five-point scale ranging from high to low, (see Exhibit 1). When assigning a credit rating we consider cyber risks in the context of all other risks an issuer faces. A significant cyber event could lead to lower scoring for factors such as cost structure, market position, profitability, coverage and leverage. When we believe an emerging risk is highly likely to weaken a company's credit quality, we incorporate these expectations into our ratings. Consistent with this long-standing approach, we expect to incorporate the credit effects of cyber risk as our understanding of issuer-level exposures and mitigation strategies evolves and well before the effect of a significant cyber event is fully evident in financial and operating results.

Exhibit 1

## Cyber risk factors and assessment levels



Source: Moody's Investors Service

### Credit implications of high-profile cyberattacks

Several rated debt issuers have been hit with cyberattacks that have weighed on their operating performance and created reputational issues. Although the costs of attacks can be significant and there has been at least one case in which we downgraded a company's rating following a cyber breach (see [Moody's downgrades Altegrity's CFR to Caa3; outlook negative](#), September 12, 2014), the highest-profile events have yet to result in any material deterioration in the creditworthiness of affected companies. However, the frequency and magnitude of attacks could weaken the credit quality of the most-exposed entities in the coming years.

In one of the biggest episodes to date, Equifax Inc. announced in September 2017 that a data breach had compromised the personal information of about 143 million US consumers, plus a limited number in Canada and the UK. The breach was unprecedented in terms of the number of consumers affected and the personally identifiable information that was compromised. Since the incident, the company has been defending itself against hundreds of lawsuits. The company is also subject to investigations by federal and state regulators.

Two other rated issuers, [FedEx](#) (Baa2 stable) and [Merck & Co., Inc.](#) (A1 stable), were among the companies hit by the NotPetya ransomware attack in 2017, which collectively resulted in an estimated \$10 billion in global financial impact across all of the affected entities. Ransomware attacks, which seek to block access to an organization's critical data or systems, are a type of disruptive attack that have become increasingly widespread. Although the initial intent of ransomware may be financial gain through solicitation of a ransom paid to unlock systems or data, there is no guarantee that the attackers will return access even if an organization complies.

[Marriott International, Inc.](#) (Baa2 stable) disclosed in November 2018 that its Starwood guest reservation database had been breached, with potential impact on as many as 500 million guests. The episode raised the potential for direct costs associated with the investigation into the breach, as well as any litigation or liability that Marriott may face with respect to compromised data. In the wake of the breach, Marriott stated that it carries cyber insurance and is working with its insurers to determine coverage.

Exhibit 2 shows some of the most notable cyberattacks on rated issuers in recent years and the extent of the impact.

Exhibit 2

#### A number of rated issuers have faced cyberattacks in recent years

Issuer	Date	Description	Impact
<b>Marriott International Inc.</b>	November 2018	Breach of Starwood guest reservation database, with potential impact on 500 million guests who made a reservation at a Starwood property. Breached data included names, addresses, credit card numbers, phone numbers, passport numbers, travel locations and arrival and departure dates.	The attack had no immediate impact on Marriott's ratings or outlook. Key risks from the breach included the potential for direct costs associated with the investigation into the attack, as well as any litigation or liability that Marriott may have with respect to compromised data. Long-term risk may include potential guest concerns about staying at a Marriott property as Marriott and Starwood merged their rewards program in August 2018.
<b>Bank of Montreal and Canadian Imperial Bank of Commerce</b>	May 2018	Both entities were contacted by parties claiming to possess personal and financial information pertaining to 50,000 BMO clients and 40,000 clients of CIBC's direct banking affiliate, Simplii. Neither bank made any payment.	There was no indication that any client suffered a financial loss, but the reputational risk to the banks from such a financial data security breach was credit negative.
<b>Equifax Inc.</b>	September 2017	Unauthorized intrusions through its consumer-facing website applications resulted in criminals accessing personally identifiable information such as names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. The breach affected roughly 143 million US consumers, plus a limited number of consumers in the UK and Canada.	Since the incident was disclosed, Equifax has reported \$440 million in costs net of insurance recoveries. Longer-term risk stemmed from whether the breach would cause lasting harm to Equifax's reputation and any potential effect on its relationships with customers.
<b>FedEx Corporation</b>	June 2017	The worldwide operations of its TNT Express subsidiary were significantly affected by a cyberattack. The attack did not affect the systems and data of any other FedEx companies.	The attack negatively affected Express segment results in fiscal 2018 by about \$400 million, primarily from loss of revenue resulting from a pause in shipments and incremental costs to restore network IT systems. Effects from the attack, such as lost volumes, lingered, although most of the revenue base later returned.
<b>Merck &amp; Co., Inc.</b>	June 2017	A cyberattack led to the temporary disruption of the company's worldwide operations, including manufacturing, research and sales functions.	The attack exposed Merck to incremental costs as it restored operations; however, the company's strong credit metrics and positive operating momentum somewhat offset the negative impact. A strong financial profile provided cushion to absorb costs associated with the attack and the temporary disruptions.
<b>Tesco Personal Finance Plc</b>	November 2016	A cyberattack affected more than 8,000 personal current accounts. The attack was a mass-algorithmic fraud attack and did not involve any loss of customer data.	The UK's Financial Conduct Authority fined the company £16.4 million for shortcomings related to the cyberattack.

Source: Moody's Investors Service

## Sector-level risk assessments

We classify four sectors as high risk in terms of their overall cyber risk. Collectively, the companies in these sectors have total rated debt outstanding of \$11.7 trillion. These sectors are banks, securities firms, financial market infrastructure providers, and hospitals, all of which have a significant reliance on technology and confidential information for their operations.

Nine sectors are at medium-high risk and have total rated debt outstanding of \$8.9 trillion. They include electric utilities, retail, technology, telecommunications/media and manufacturing (including automobiles and medical devices). These sectors rely heavily on technology and data to operate but have some ability to offset impact through distributed revenue channels or geography, or, in some cases, manual process alternatives.

The 11 sectors we assess as medium risk have total rated debt outstanding of roughly \$3 trillion. These sectors include public infrastructure providers (ports, airports and mass transit), asset managers, property & casualty (P&C) insurance companies (excluding health insurance) and pharmaceuticals. These sectors have fewer direct touchpoints with end consumers or they have demonstrated that they can use manual processes during business disruption events.

Seven sectors with a total of \$46.5 trillion in outstanding rated debt are medium-low risk. They include sovereigns, which account for \$35 trillion of the debt, and other government issuers, and less-digitized sectors such as consumer products, oil & gas, and structured finance.

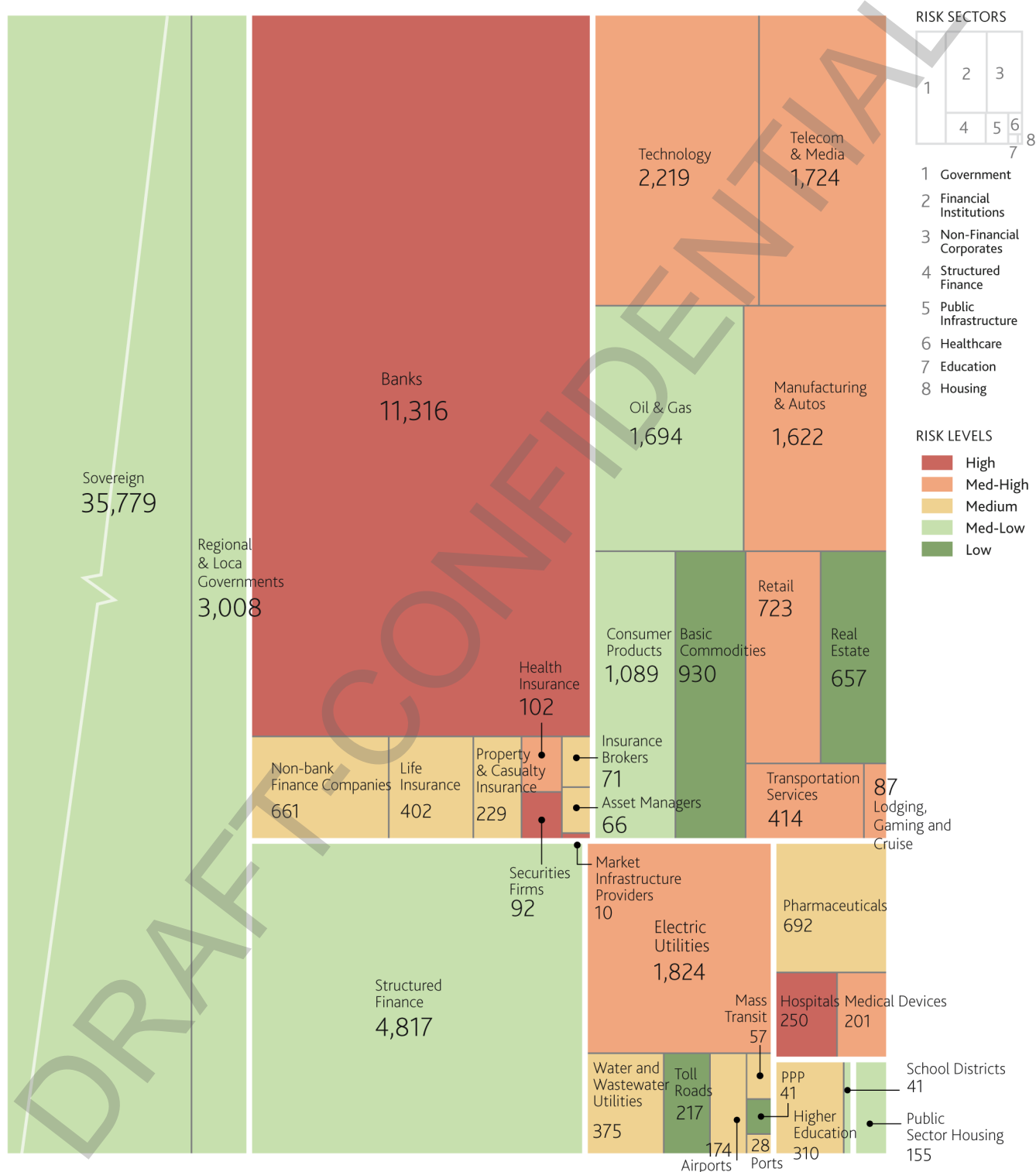
The four low-risk sectors are basic commodities, public-private partnerships, real estate and toll roads, which collectively have \$1.8 trillion of total rated debt outstanding. These sectors have little reliance on interconnected technology and often operate with limited competition.

Exhibit 3 shows our classification of 35 sectors assessed in this study and their relative sizes.



Exhibit 3

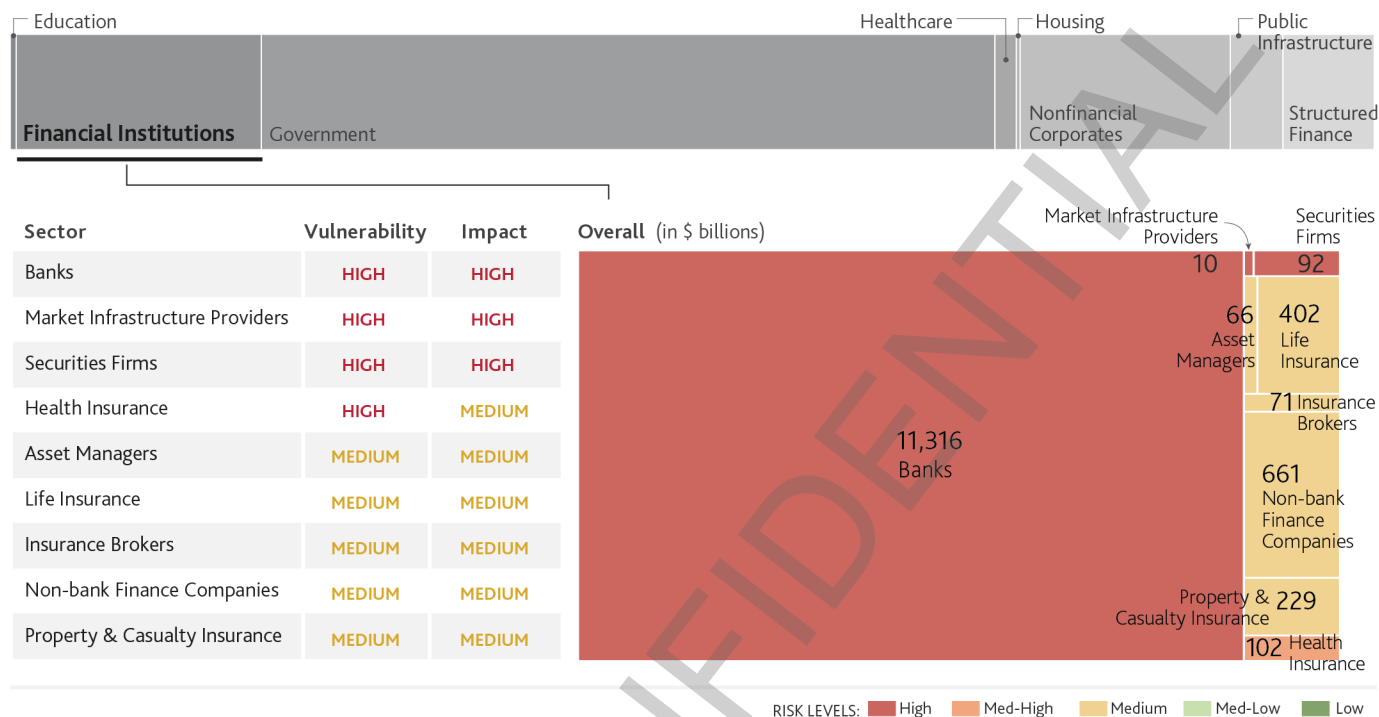
## Cyber risk levels and Moody's-rated debt (in \$ billions)



Data on outstanding debt includes Moody's-rated debt only. For rated sovereigns, debt outstanding totals \$60.5 trillion when including both rated and unrated debt.

Source: Moody's Investors Service

## Financial Institutions



The financial sector has significant cyber risk exposure. Banks are at high risk because they hold the data and funds of private clients, and they provide access to their services through multiple online and digital channels. Securities firms, including capital markets firms, are also at high risk: they are appealing targets for cyber criminals aiming to carry out large-scale theft as well as sophisticated attacks designed to create operational disruption or garner publicity. A successful attack on large, systemic banks could pose a systemwide risk, reflecting their high degree of interconnectedness. Similarly, successful cyberattacks against financial market infrastructure providers such as exchanges and clearing houses, or counterparties such as large securities or capital markets firms, could impair the booking, clearing and settlement of financial transactions. Non-bank finance companies are at medium risk: their business models are diverse and expose them to a large spectrum of cyber risks.

Both large and small financial institutions are subject to a large volume of attacks. Smaller institutions with fewer resources and less developed risk-management infrastructure could be more exposed to attack and less able to mitigate the risk. However, large institutions are at greater risk of sophisticated cyberattacks designed to steal or manipulate data, to create significant operational disruption, or simply to generate negative publicity.

Banks and other financial institutions have been investing heavily to enhance their monitoring and risk mitigation capabilities in this area. In addition, the industry increasingly conducts exercises in which in-house experts attempt to hack systems so as to identify potential vulnerabilities. Information-sharing between financial institutions regarding attempted attacks has also increased. This is a clear benefit for an industry that is highly interconnected and prone to contagion risk.

The insurance sector is information-rich and interconnected, with a dependency on vast quantities of personal, commercial and financial information for its core processes. Insurers also interact broadly with individuals, businesses and government enterprises, as well as capital markets and regulatory functions, which creates vulnerabilities. For example, many jurisdictions mandate coverage for automobile, homeowners', and employer and professional liability insurance. Lenders and securitization markets also may require such insurance coverage. Insurers possess potentially sensitive personal health, income, asset and lifestyle information, as well as financial and operational data for businesses, governments and other institutions, which creates significant cyber-related exposure. Some large insurers have capital markets activities and interdependencies that create additional sensitivities.



One especially notable cyber-related consideration for the sector is the growing significance of the cybersecurity insurance market, a small but rapidly expanding product segment for commercial insurers and reinsurers. This coverage effectively transfers significant amounts of cybersecurity risk from individuals, businesses, and governments to the insurance sector, which helps alleviate financial risk for those sectors but increases risk for insurers. This accumulation risk could have significant impact if a successful attack affected a shared technology provider that a large number of insured entities use. The anticipated growth of connected devices (the “internet of things”) in insured cars, homes and businesses, as well as health and fitness, manufacturing and surveillance technologies, is another consideration for the insurance sector.

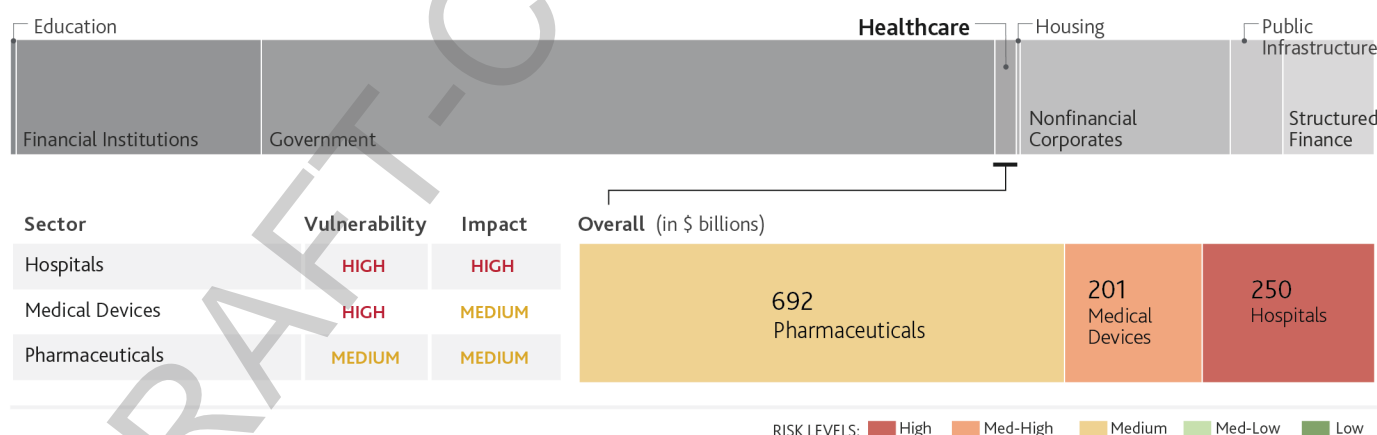
### Financial institutions lead the pack in terms of regulation

International standard setters and regulators are putting more emphasis on cyber risk management and monitoring for financial institutions. The most relevant international standards are the CPMI-IOSCO guidance for cyber resilience of financial market infrastructure providers, the NIST framework and the ISO 27000 series.

Among regulators, the Bank of England launched a framework in 2014 to help identify areas where the financial sector could be exposed to sophisticated cyberattacks, and in 2018 it updated its CBEST framework to test firms' cyber resilience. In 2017, the Federal Financial Institutions Examination Council (FFIEC) updated the FFIEC Cybersecurity Assessment Tool to help institutions identify risks and assess preparedness. In 2017, the New York State Department of Financial Services introduced new requirements on cybersecurity.

In May 2018, the US Congress mandated the US Department of the Treasury to report within a year on the risks of cyber threats to US financial institutions and capital markets, and on how the federal banking agencies and the Securities and Exchange Commission are addressing these material risks. It also requested a recommendation as to whether any additional legal authorities or resources are needed. In November 2018, the Australian Prudential Regulatory Authority finalized a prudential standard relating to cyber risk management. However, regulatory reaction has been inconsistent globally.

## Healthcare

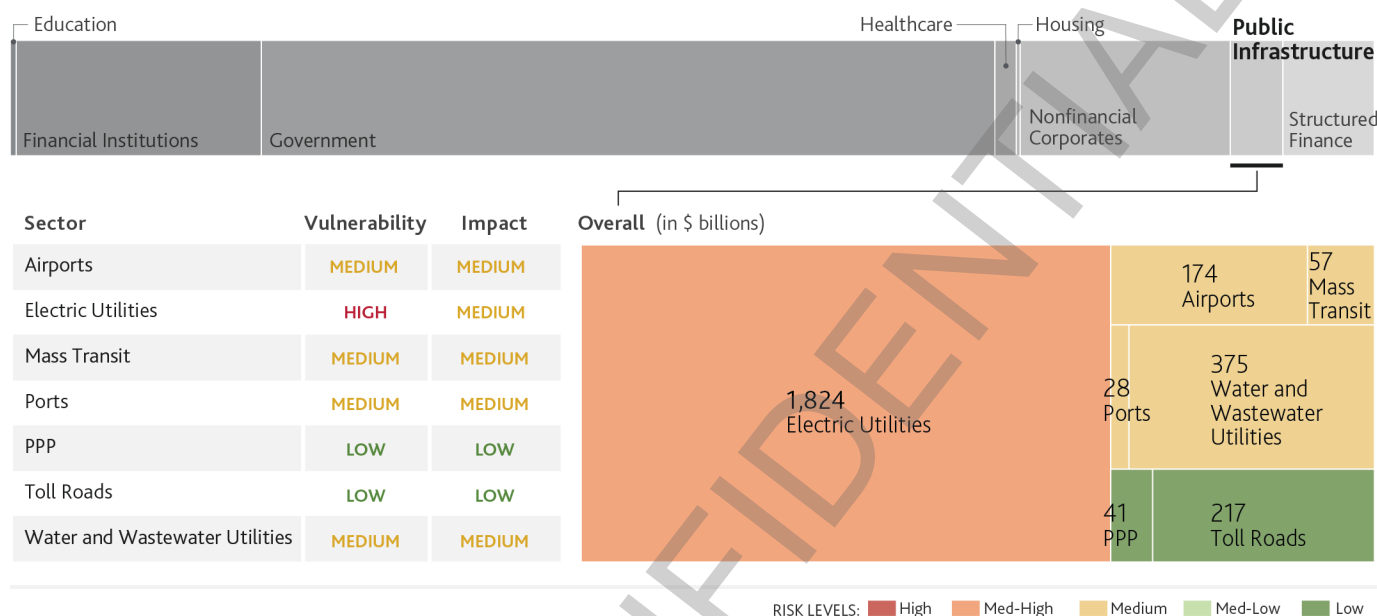


The healthcare sector comprises the primary subsectors of hospitals, pharmaceutical companies and medical device manufacturers. Each industry has somewhat different cyber risk profiles that reflect their relative vulnerability to an attack and the impact of a successful attack.

For hospitals, our assessment primarily reflects the sensitive and essential nature of the data collected and used by these entities and its attractiveness to hackers, as well as vulnerabilities emanating from increasingly connected medical devices. For medical device manufacturers, devices such as insulin pumps, defibrillators or cardiac monitoring are now in widespread use and increasingly rely on remote monitoring, which creates vulnerabilities. For pharmaceutical companies, our view is that, while these companies do store

proprietary data and information that may be a target for theft, it is highly unlikely that such information could be used to develop a rival drug given regulatory standards and oversight of the approval and distribution processes.

## Public Infrastructure

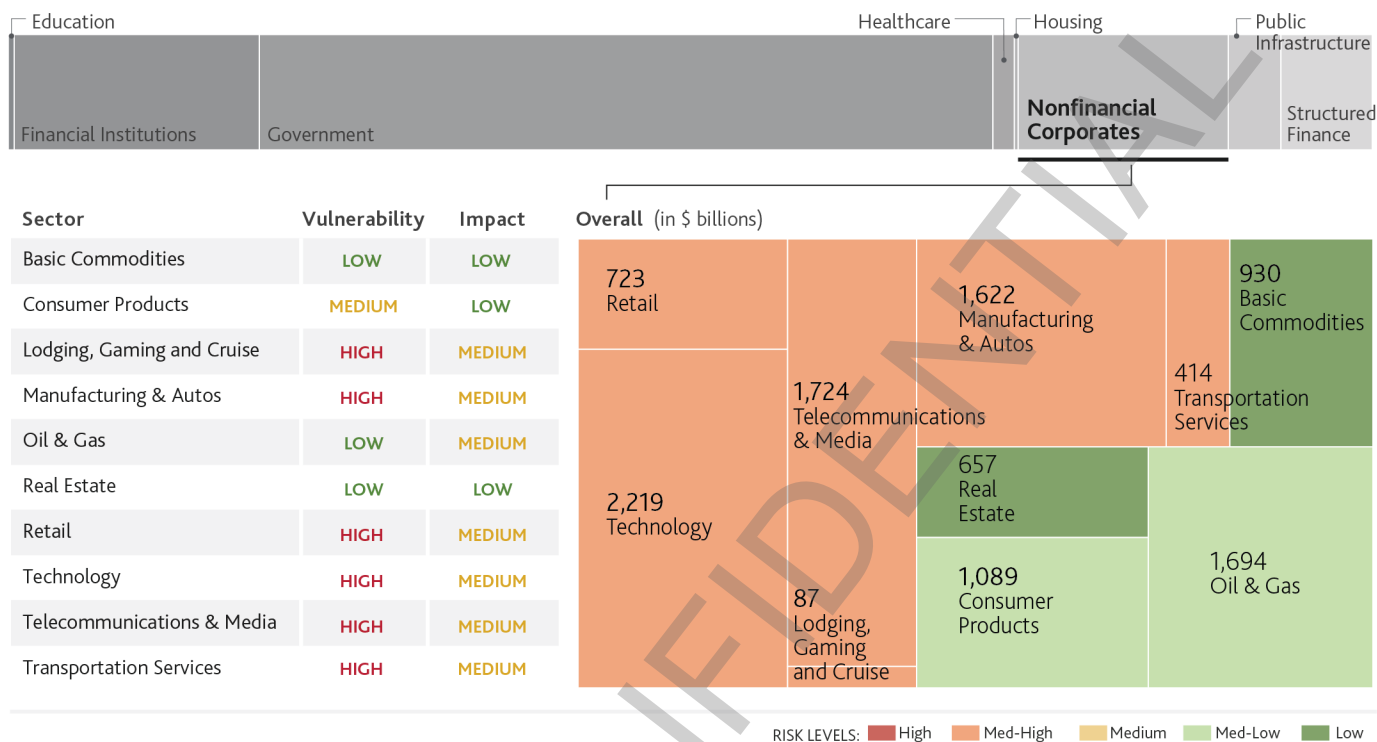


Overall we view public infrastructure's exposure to cyber risk as medium-high because electric utilities account for a considerable portion of the rated debt in the sector. However, the extent of the respective industries' digitization, the ownership and revenue model that applies, and the broader economic impact of any service disruption will greatly influence the score of individual infrastructure sectors.

Although the market and ownership structure of electric utilities varies significantly across regions and countries, we have opted to group them together for practical purposes and to reflect the highly integrated nature of these different market participants. As a result, this category includes not only regulated electric and gas utilities, but also standalone regulated networks, unregulated utilities, power generators and US public power utilities. In practice, the vulnerability of an electric utility to a cyberattack and the impact of the attack will vary depending on a given company's ownership and market structure.

For both electric utilities and transportation, cyber risk primarily stems from intent to disrupt or destroy service, rather than a profit or public relations motive. Transportation industries are typically less integrated and digitized than electric utilities, and consequently are less exposed. Although the number of reported successful cyberattacks on public infrastructure has been growing rapidly, none has resulted in a rating change to date. However, the frequency and magnitude of attacks could weaken the credit quality of the most exposed entities as issuers struggle to keep up with the rapidly improving capabilities of threat actors around the world. Private public partnerships (PPPs) are a financing structure that can include assets in the utilities or transportation sectors, but they can also cover a wide number of other sector types as discussed in the appendices.

## Nonfinancial Corporates



Overall, the nonfinancial corporate sector is subject to a range of cyber risk exposure from medium-high to low. This assessment masks wide disparities among industries. The most-exposed segments have highly technological operations, frequent interactions with end customers, or both. Together, these features create risks of disclosing private information or banking data and therefore reputational risk. In addition, many companies with heavy investments in research and development are subject to data theft. Lastly, targeted attacks can severely disrupt companies with complex supply chains. Although cyber risk has not yet led to any significant change in a company's debt ratings, the growing frequency and magnitude of attacks could weaken the credit quality of the most exposed companies in the coming years.

The companies most exposed to cyberattacks operate in technology, telecommunications and media, lodging, gaming and cruise, manufacturing and autos, transportation services and retail. Consumer goods and oil & gas have a medium-low exposure to cyber risk. Targeted attacks on critical systems such as aircraft, autonomous vehicles or pipelines could cause material liabilities, although the distributed nature of the end user base or the lack of widespread adoption of new technologies would somewhat mitigate the harm.

### Data privacy regulations and government protections

More than 100 countries have implemented or are in the process of passing some form of data privacy and protection legislation. While not directly targeting cyber risk, they are generally focused on setting standards for the collection and safe handling of individuals' personal information, as well as providing prohibitions on the disclosure or misuse of such data, a key source of cyber risk. In addition, these measures may include financial penalties, which can add to the costs of data breaches where companies are found liable.

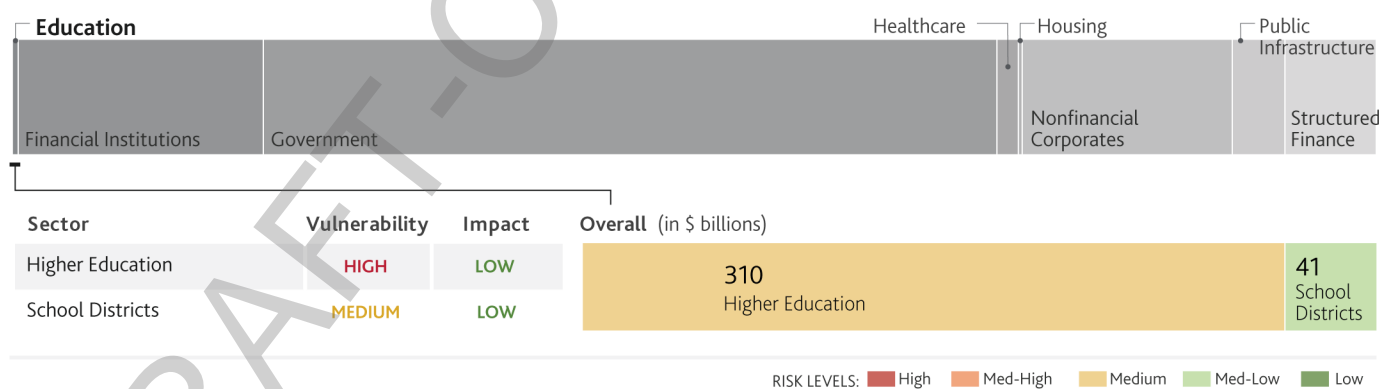
Examples include:

The European Union's **General Data Protection Regulations** (GDPR): Perhaps the most high profile of recent initiatives, the regulations hinge on the core tenet that individuals have a right to complete control over the data that is collected, and to know who collects the data, what is done with it and how their online activity is used more generally. The potential fines allowable under GDPR can range up to the higher of €20 million or 4% of global annual turnover.

In the US, there is no overarching federal privacy regulation, but there are a number of sectoral and state laws. With regard to the former, one example is the **Health Insurance Portability and Accountability Act of 1996** (HIPAA). While initially focused on improving efficiency and speeding the transfer of patient data, recent amendments to HIPAA have focused on restricting the use and disclosure of patients' data and health information. Fines for violation of HIPAA rules can range from up to \$50,000 per patient to criminal prosecution. At the state level, Massachusetts and California are widely considered as having the most stringent rules. In addition to setting out what constitutes personal information and how it should be handled, Massachusetts also stipulates what constitutes a comprehensive information security program as well security requirements for businesses' computer systems.

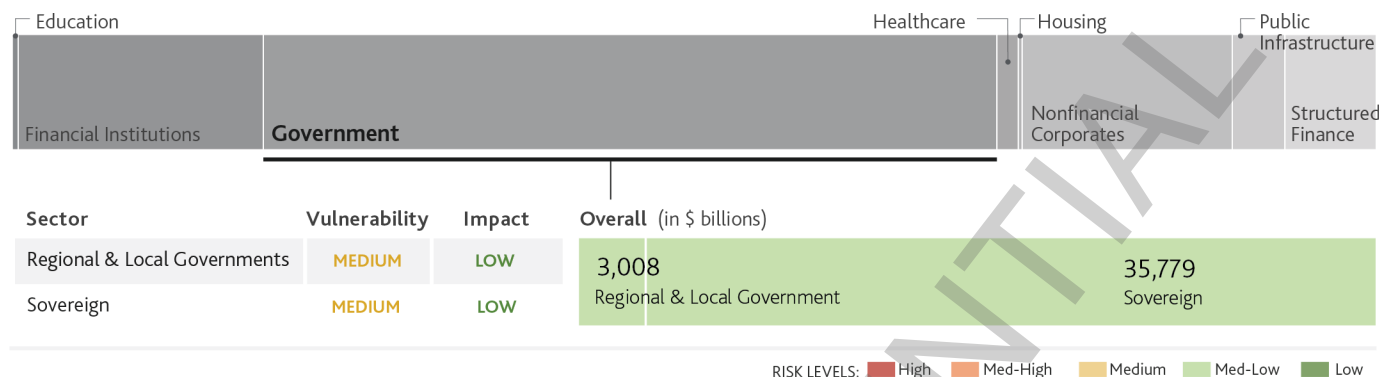
Japan's updated privacy law – the **Act on the Protection of Personal Information** (APPI) – came into effect in 2017. Its approach and key tenets are similar to those of the GDPR, with the core focus on protecting the rights and interests of individuals by ensuring that they are informed about what information is being collected and for what purpose, and that entities that collect the data handle it properly. Fines for the misuse of personal information range from up to ¥500,000 to one year in prison.

### Education



The education sector spans higher education (US and subsovereign) and school districts. The higher education sector is vulnerable to cyberattacks because the information it retains is considered highly valuable for businesses and governments. This is particularly true for large, research-intensive universities with academic medical centers as they conduct research that is often highly sensitive and retain significant medical records, therefore owning the most sensitive data in the sector. Additionally, vulnerability to cyberattacks increases as universities engage in academic and research partnerships around the globe. Cyber breaches could result in reputational damage to an institution, lowering its ability to secure enrollment, funding and research staff. This in turn could reduce an institution's competitiveness. Meanwhile, for US school districts, a severe breach could expose personal data about students and their families, programs that relate to financial status, and academic and medical information.

## Governments



The government sector spans sovereign, subsovereign regional and local governments (including US states). Although each subsector has variation, larger government entities tend to have higher public profiles, more substantial resources and revenue bases, and control over highly sensitive or confidential information. These features make larger government entities targets for cyberattacks. For example, criminals have attempted to disrupt essential government services, as demonstrated by attacks in Estonia, Ukraine and Finland in recent years, or have tried to access sensitive information, such as the theft of US government employees' classified information. Cybersecurity attacks on central banks in Bangladesh and Mexico indicate some attacks are also financially motivated.

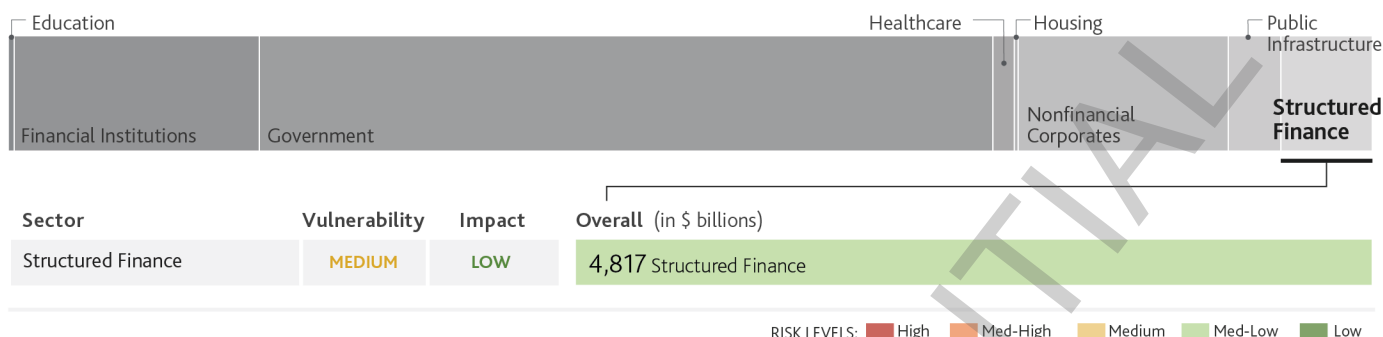
Our overall assessment of cyber risk for government entities is medium-low, driven by generally higher vulnerability scores that are mitigated by lower impact scores. Although the threat profile of large government entities is higher relative to smaller local governments, this assessment is mitigated by generally stronger defense profiles as a result of dedicated and effective cybersecurity resources. While many sovereigns are high-profile targets, they have strong cyber defenses. Combined with the large scale and diversified nature of their economies, these cyber defenses mitigate the potential impact of cyber risks.

## Housing



For social housing providers, disruptions to rent payment or government transfers present the largest risk but are less likely to have an impact because of the presence of manual alternatives. We expect potential cyberattacks that leak data to be more probable, because the social housing sector retains personal data for a substantial proportion of a given population. There are high levels of demand for social housing globally, which helps mitigate a reduction of the customer base. While IT investment has increased as a means of delivering cost efficiencies, few rated entities in the sector are addressing cyber risk concurrently. Social housing providers typically have strong balance sheets and liquidity buffers that can mitigate revenue loss, as well as strong links with their respective governments, which provide an additional level of support.

## Structured Finance



Allowing for some variation across sectors, the risk to structured finance transactions from cyberattacks is medium-low overall. Although some transaction parties may be in sectors that have a high exposure to cyber events (a bank lender that sponsors a transaction, for example), the legal separation of the structured transaction and the assets' originator dilutes the risk that an attack on an originator will significantly harm the cash flow that the underlying assets generate.

A cyberattack that affects a sponsor's operational ability or credit quality can have some impact on a structured transaction's performance in some cases, such as those in which the sponsor retains some responsibility related to the assets (for example, by continuing to service the accounts). However, the likelihood of such a disruption lasting long enough to have a significant credit impact on the transaction is low. The dependence of structured transactions on third-party entities adds to their vulnerability. These third parties include servicers, trustees and other administrative entities, such as paying agents, calculation agents and custodians. But mitigants such as minimum counterparty rating requirements, coupled with transfer provisions, add to the durability of transaction service providers. Servicers also often have backups to protect against operational disruptions from catastrophic events including cyberattacks, which serve as a significant risk mitigant.






## Appendix I: Summary of high-risk sectors

*These sectors have a significant reliance on technology and confidential information for their operations and are highly interconnected, both internally and externally. As a result, they will often have a limited ability to fall back on manual operations, either because of the nature of their business or because they are unable to do so efficiently while remaining competitive. These sectors also often represent critical global infrastructures that are both data rich and where even short-term disruption would have a cascading and far-reaching impact on other sectors (for example, banks and hospitals).*

### Financial Institutions

#### Banks

	OVERALL High	 VULNERABILITY: High  IMPACT: High	\$11,315.9 billion Rated debt
---	-----------------	---	----------------------------------

Retail banking is a daily target for cyberattacks. Banks not only house coveted private client data and deposit funds but they also provide access to credit and account information through online and mobile channels while handling credit card-based transactions. Data is integral to the franchise strength of retail banks, since it underlies underwriting, customer records and business development. An attack that managed to impair the functioning of payment systems and processes – for example, Fedwire, BACS or TARGET2 – would cause major disruption and potentially unsettle the entire economy. Vulnerabilities stem from the networks that connect customers to banks and vendors.

Moreover, since vendors typically provide services to numerous financial institutions, an undetected attack on a single vendor could affect a group of retail banks. Less sophisticated cyberattacks are unlikely in most cases to result in data loss because banks have well-established procedures to block attacks before data is stolen or compromised and they also have processes to recover funds in the case of fraud.

The wealth management industry is an attractive target for cyber criminals because it serves high-net-worth individuals. The consequences of customer data loss can be severe in this business, as clients typically attach high importance to data integrity and privacy. Further, high-net-worth individuals often use multiple service providers, making it easier for them to switch providers if necessary.

Corporate banking is a less likely target than other bank businesses because of the wholesale nature of the activities. Vulnerability stems mainly from the fact that these operations provide critical payment and cash management services to clients. However, corporate banks do not house private client data, making them less attractive targets than retail banks. Corporate banks' long-term relationships with clients, together with the high replacement cost of infrastructure linking banks to their corporate clients, also mitigate the potential loss of clients if attacks cause operational disruption.




#### Securities Firms

	OVERALL High	 VULNERABILITY: High  IMPACT: High	\$91.8 billion Rated debt
---	-----------------	---	------------------------------

Large securities and capital markets firms, whether independent or controlled by a banking group, could be appealing targets for cyber criminals aiming to carry out large-scale theft, and could also be targets of sophisticated attacks designed to create operational disruption or generate publicity. As with retail banks, securities firms serving retail clients house coveted client data and provide access to account information through online and mobile channels while they also handle securities transactions. An attack that leads to the loss of client funds or a denial of service for several days could cause considerable franchise damage.

Cyberattacks on large and high-profile capital markets and securities firms and businesses could pose systemwide risk. An attack that impairs the functioning of settlement, payment or clearing systems would cause major disruption to the financial markets and would likely unsettle the entire economy, given the high interconnectedness between capital market participants and market infrastructure providers.

## Market Infrastructure Providers




 OVERALL High	 VULNERABILITY: High  IMPACT: High	\$10.4 billion Rated debt
---	---	------------------------------

Highly interconnected financial institutions, including exchanges and clearing houses with considerable reliance on technology platforms, are at risk of sophisticated attacks designed to create economic and social disruption or to generate publicity. A successful cyberattack would likely cause major disruption.

However, market infrastructure providers are generally well attuned to the risks of cyberattacks because operational resilience, supported by ongoing monitoring and mitigation of cyber risk, is integral to their operations and franchise security. They also devote significant resources to cyber risk management.

## Healthcare

## Hospitals

 OVERALL High	 VULNERABILITY: High  IMPACT: High	\$250.4 billion Rated debt
---	---	-------------------------------

Hospitals and laboratories are exposed to breaches of patient information and the disruption of medical procedures and technologies. Hospitals increasingly share data with various third parties, such as health insurance exchanges and other payors, necessitating the need to safeguard confidential information with modernized IT and security systems. Patient data includes confidential medical records as well as social security numbers and insurance information. As a result, a data breach could create substantial legal risk for healthcare companies. In addition, a breach of medical technology would pose an immediate threat that could harm the reputation of the hospital or lead to ransom demands.

Hospitals of all sizes will be vulnerable. Although hospitals with more financial resources will be better able to avoid threats or recover from an attack, size does not provide immunity. The electronic medical record (EMR) is the primary tool used to collect patient data from billing information, medical history, physician orders, test results and to account for any other charges incurred during a patient visit. The EMR is critical to nearly all hospitals' infrastructure and any disruption can impact operations and impair financial performance.




There are limited legal protections for hospitals, and only a small number of rated hospitals report getting cyber insurance because of its high cost. For example, in the US, hospitals and other healthcare providers are regulated under the Health Insurance Portability and Accountability Act. Under the act, protected health information that is inappropriately accessed or breached is required to be reported, which can sometimes result in fines. However, patients are unlikely to switch hospitals and often cannot do so because of a lack of alternatives in the market.

## Appendix II: Summary of medium-high risk sectors

These sectors have multiple vulnerabilities that make them cyberattack targets. They rely heavily on technology to operate, although they have some ability to reduce the operational impact of an attack through established manual processes. However, a significant data breach or prolonged disruption of operations would result in meaningful impact that reputational effects could further amplify.

### Public Infrastructure

#### Electric Utilities




 OVERALL Medium-High	 VULNERABILITY: High	\$1,824.1 billion
	 IMPACT: Medium	Rated debt

Electric utilities operate highly integrated and increasingly digitized critical infrastructure that underpins the broader economy and people's way of life.<sup>2</sup> Furthermore, the monopolistic nature of providing electric services leaves customers with little alternative access to electricity in case of an attack on an electric utility's grid. The combination of these two factors makes electric utilities attractive targets for cyberthreat actors looking to disrupt not only a particular company's services but also economic processes and quality of life.

Although electric utilities rank among the most attractive cyberattack targets, the financial and credit impact of an attack would likely be moderate. Unlike companies operating in fully competitive markets, utilities are regulated by regional or national bodies. The regulatory framework governing their operations is typically designed such that efficient utilities can recover their costs, including capital costs, within the tariffs they charge. As a result, in the event of a cyberattack that caused financial or physical damage to the physical grid infrastructure, we would expect regulators to be sympathetic to the utility being able to recover these costs, albeit potentially with a time lag, and the utility would likely avoid penalties through the regulatory framework.

### Financial Institutions

#### Health Insurance




 OVERALL Medium-High	 VULNERABILITY: High	\$101.5 billion
	 IMPACT: Medium	Rated debt

Our overall risk assessment considers health insurers' intrinsic cyber risk profile as well as the cyber sensitivities of other health-related enterprises with which they interact and exchange information. Health insurers have been among the higher-profile targets of cyber intrusions in recent years. They have extensive access to information about customers' health and medical conditions. The industry is also highly concentrated, has large transaction volume and depends on digital information and communications.

Health insurers have a significant degree of exposure to adverse reputational, financial and legal and regulatory consequences because of the sensitive nature of their customer data. The potential for operational risk is significant, arising from a sustained disruption in services, corruption of data or a compromise affecting other medical service providers with whom they interact. That said, cyberattacks generally have not resulted in any significant or sustained disruption for health insurers' finances or reputation. Additionally, and largely for these reasons, health insurers are among the most active within the sector in cyber risk management.

### Nonfinancial Corporates

#### Technology

 OVERALL Medium-High	 VULNERABILITY: High	\$2,219.1 billion
	 IMPACT: Medium	Rated debt


The technology sector remains ripe for attacks amid the proliferation of cloud services, the explosion of stored data from social networks and the internet of things, and the increasing reliance of many industries on the hardware, software and services provided by this diverse sector. Rapidly evolving technologies, access to vast troves of data, increased access points and the brand prestige of leading tech companies will continue to attract hackers. A major cyberattack would have a large effect on the reputation of peer companies within the sector. Security threats or compromises can undermine the faith of customers, who place great weight on



security considerations when purchasing products and services from tech vendors. Hackers will naturally focus on companies with the most popular products and services to maximize their potential financial gain, or their impact in the case of disruption.

We view the overall impact score as medium given that the technology industry comprises not only leading firms with very strong credit profiles and robust liquidity but also many smaller, niche software and services providers with very high financial leverage. A disruption in services, a prolonged outage or reputational damage could cause severe financial harm for these smaller companies.

To date, reported cyberattacks have had limited effects on earnings of the technology firms involved. For example, although the security breach at Equifax led to reputational harm, as well as heightened regulatory and litigation costs, the company's strong financial position and liquidity mitigated these factors. Indeed, the largest technology firms maintain the highest cash balances of any sector, by far, making these companies generally well positioned to cover revenue losses and costs associated with a major cyberattack.<sup>3</sup>

#### Telecommunications & Media

 **OVERALL**  
Medium-High

 **VULNERABILITY:** High  
 **IMPACT:** Medium


\$1,723.9 billion  
Rated debt

New technologies and services will increase the entry points and opportunities for cyberattackers. Similarly to cloud providers, network operators will be exposed to the most sophisticated cyberattackers. Large social media sites, such as Twitter and Facebook, are typically large data gatherers with significant private information. Breach of private information entrusted to a social media platform or malicious political influence on political campaigns could have damaging effects on brand and customer loyalty. However, the size of the platform and its entrenched user base may limit the potential impact, as recently seen with Facebook. For media content companies, significant intellectual property is at risk of release before it is commercially exploited.

For telecom companies, cyber espionage has also received greater attention with the recent debates regarding the ability of telecom equipment manufacturers to aid government surveillance. As an example, speculation that hardware could be subverted during the assembly or manufacturing process is creating growing concerns with the build-out of next generation 5G wireless networks. This technology is likely to facilitate the use of virtual reality, autonomous cars and the internet of things.

Although the telecom sector has high vulnerability to cyber events, we view the impact as medium because large carriers are best positioned against cyberattacks. [AT&T](#) (Baa2 stable) and [Verizon](#) (Baa1 stable), for example, have large volumes of network traffic while serving many government agencies across different jurisdictions. Accordingly, these carriers are required to develop, implement and maintain rigorous network capabilities and standards. They also collect and store data for government surveillance activity in domestic and international markets. Smaller carriers with less sophisticated security capabilities but which still handle large volumes of traffic are more vulnerable. The more that the network's architecture is centralized, the more it is at risk of a disruptive attack. However, a service outage is likely to be localized and more containable for small carriers that operate with a smaller geographic footprint.

#### Retail

 **OVERALL**  
Medium-High

 **VULNERABILITY:** High  
 **IMPACT:** Medium




\$723.3 billion  
Rated debt

As the high-profile data security breaches at Target, [eBay](#) (Baa1 stable), [Home Depot](#) (A2 stable), and [Neiman Marcus](#) (Caa3 stable) illustrate, hackers will continue to attack retailers for credit card and debit card information. For those merchants that process card payments and store sensitive merchant and consumer information, data theft can lead to claims against the companies, the loss of market reputation and potential regulatory scrutiny. In addition, denial of service could prevent point-of-service or e-commerce retailers from fulfilling customer purchase orders, a major risk for retailers. In many cases, the timing of a cyber event could have a larger impact on a retailer than on other types of companies because of the seasonality of the business.

We view impact as medium because many companies, such as eBay, have overcome significant breaches without material business disruptions. But the fallout from a cyberattack can compress already thin profit margins. There are the direct costs of the breach itself (for example, litigation and technology remediation costs), as well as the effect on customer satisfaction, which can be harder to measure. Smaller retailers have more exposure to these costs because of their more limited financial resources and IT capabilities.




Restaurants, a subsector of retail, have some ability to fall back on more manual processes of revenue collection in the event of an attack, although they are highly digital with integrated point-of-sale systems. Technology is playing a larger role for restaurants as they look to drive their businesses through mobile applications, delivery technology, and data analytics and loyalty programs.

#### Transportation Services

 <b>OVERALL</b> Medium-High	 <b>VULNERABILITY:</b> High	 <b>IMPACT:</b> Medium	<b>\$414.0</b> billion Rated debt
---	--	---	--------------------------------------




A direct attack could have a disruptive effect on companies that rely on global technology systems to conduct their operations. For instance, shipping company [A.P. Møller-Maersk's](#) (Baa3 stable) systems were infected by the malware NotPetya in 2017, causing a loss that management estimated at \$250-\$300 million. For the largest airlines, vulnerability is high, while the risk is medium for smaller airlines because of differences in revenue and scale and the proportionally smaller volume of and reliance on technology for transactions or customer engagement. A cyberattack directed at an aircraft could have major consequences for airlines. Service interruptions leading to delayed or canceled flights are another source of risk. However, a denial of service attack would likely be short-lived and handled in a similar manner to normal interruptions. An outage will not typically cause customers to stop using an airline, particularly when the cause is an external factor.

#### Medical Devices

 <b>OVERALL</b> Medium-High	 <b>VULNERABILITY:</b> High	 <b>IMPACT:</b> Medium	<b>\$201.3</b> billion Rated debt
---	--	---	--------------------------------------

Our risk assessment is based on the fact that medical devices such as insulin pumps, defibrillators and cardiac monitoring are now quite widely used in remote monitoring, providing patients and their caregivers with valuable real-time information. In 2017, the US Food and Drug Administration recalled about 500,000 pacemakers because of fears that lax cybersecurity could be hacked to run down the devices' batteries or even alter the patient's heartbeat.




#### Manufacturing & Autos

 <b>OVERALL</b> Medium-High	 <b>VULNERABILITY:</b> High	 <b>IMPACT:</b> Medium	<b>\$1,622.2</b> billion Rated debt
---	--	---	--

The industry is made up of some very big companies with considerable resources that threat actors could target. Cyber risks also stem from a reliance on IT systems to control production, process data and manage customer and supplier relationships. Interruption of operations, damaged goods or theft of confidential data could lead to a loss of output and reputational impairment. The high degree of reliance on integrated supply chains provides multiple channels for cyberattacks. However, the financial impact of an attack would be low to medium given the short period of disruption that would ensue as manufacturers reroute activities to other unaffected plants, with little impact on revenue collection. Nevertheless, an attack that results in a faulty product getting into the market could lead to expensive recalls from both a cost and reputation basis.

Meanwhile, for automakers, software is playing an increasingly important role in the "connected car," which could usher in new cyber risks. A driverless car hijacked by an attacker could create significant liabilities and reputational losses.

#### Lodging, Gaming and Cruise

 <b>OVERALL</b> Medium-High	 <b>VULNERABILITY:</b> High	 <b>IMPACT:</b> Medium	<b>\$86.6</b> billion Rated debt
---	--	---	-------------------------------------

Lodging, gaming and cruise companies are vulnerable to data security breaches because of the large amount of personal data these companies maintain in their loyalty programs and reservation systems. These systems contain information including social security numbers, payment information, and driver's license or passport information. The databases for lodging companies also potentially contain sensitive information about government employees that travel for government business. A breach similar to Marriott's recent

incident could have an impact on a company's brand, but longer term we think there is enough stickiness for the customer that the brand impact will be minimal.

We view the impact as medium-high because although the impact to the brand, or financial impact from potential lawsuits, are moderate, these companies are heavily reliant on internet-based computer systems for day-to-day activities: from the software used to run the casino floor, to a hotel's booking system, to a cruise ship's navigation system. Any long-term disruption to these systems could materially harm a company's operations.

DRAFT-CONFIDENTIAL






## Appendix III: Summary of medium-risk sectors

Digitization heightens the cyber risk exposure of these sectors, but fewer external interconnections and localized operations (for example, factories) compared with higher-risk sectors somewhat offset the risk. In the event of a successful attack, these characteristics could limit the extent to which the attack spreads throughout operations. As issuers in these sectors further increase their digitization, their cyber risk profiles could increase in the next few years.

### Financial Institutions




#### Non-bank Finance Companies

 OVERALL Medium	 VULNERABILITY: Medium	\$660.6 billion
	 IMPACT: Medium	Rated debt

The business models of non-bank finance companies are diverse and show different degrees of vulnerability to cyberattacks. Consumer lenders, including credit card companies and online lenders, are subject to a high degree of cyber risk because they hold large and sensitive personal data. Some fintech lenders are highly vulnerable to cyber risk because they rely entirely on big data for their underwriting, hold large volumes of sensitive personal data and also rely heavily on the continuity of their IT systems. Leasing companies, in contrast, have lower exposure because they do not house as much personal data and their websites are not as trafficked, making them less interesting targets.

Other finance companies focused mainly on business-to-business products and services are less vulnerable to cyber risk and therefore have more moderate financial and reputational risk. They mostly rely on a small number of key relationships and suppliers, which are less likely to take their business elsewhere than are the retail customers of traditional banks.

#### Asset Managers

 OVERALL Medium	 VULNERABILITY: Medium	\$65.9 billion
	 IMPACT: Medium	Rated debt




Asset managers play a vital role in the global capital markets, which makes them an attractive target for cyber criminals. Although customer assets reside at custodian banks and therefore are not held directly by asset managers, there could be monetary loss from delayed or halted trading if a cyberattack disrupts operations. A widely publicized breach could also lead to the loss of assets, especially given the industry's increasing competitive pressures and relatively low switching costs.

#### Property & Casualty Insurance

 OVERALL Medium	 VULNERABILITY: Medium	\$229.1 billion
	 IMPACT: Medium	Rated debt

P&C insurers and reinsurers possess protected personal and commercially sensitive information and have significant interdependencies with government, businesses and capital market participants. P&C insurers have significant potential for cyber-related operational disruption. Our assessment also considers a unique characteristic of the sector: the risk assumption of the financial consequences of policyholders' cyber risk exposures through policy contracts. Cyber-related insurance coverage exposures remain modest overall compared with the size of P&C insurers' total operations, but customer demand for coverage and the scope of provided coverage continue to expand rapidly. Claim frequency and severity also continue to increase rapidly for insured clients. Although insurance typically absorbs only a small percentage of the total economic impact of a cyber event, insurance is becoming increasingly significant.




#### Life Insurance

 OVERALL Medium	 VULNERABILITY: Medium	\$401.8 billion
	 IMPACT: Medium	Rated debt

Our assessment considers the moderate degree of sensitivity of the personal information these insurers possess and their high degree of digital electronic connectivity. In many cases, life & annuity insurers have significant capital market interdependencies related to

their asset management and derivatives activities. They have extensive access to clients' personal data, some of which may constitute sensitive or otherwise legally protected information. These insurers are among the largest institutional asset managers, which makes them potentially high-profile targets. As underwriters of often long-term insurance and as significant participants in institutional pension funds and capital markets, they have significant reputational risk and notable credit and confidence sensitivity. They have exposure to legal and regulatory risk in the event of the unauthorized disclosure of sensitive client data. Cyber-related disruptions of asset management and derivative product activities could be operationally disruptive.




#### Insurance Brokers

 <b>OVERALL</b> Medium	 <b>VULNERABILITY:</b> Medium  <b>IMPACT:</b> Medium	<b>\$70.9 billion</b> Rated debt
--	---	-------------------------------------

Insurance brokers provide businesses, institutions and governments with advice and solutions regarding property and liability risks including cyber as well as employee benefits. Through their placement of insurance policies and benefit plans, brokers handle commercially sensitive information and have significant interdependencies with insured clients and insurance carriers. This exposes the brokers to cyber-related disclosure risks and operational disruption. They also face reputational risk given their role in advising clients on cyber risk management and insurance coverage.

#### Education

##### Higher Education




 <b>OVERALL</b> Medium	 <b>VULNERABILITY:</b> High  <b>IMPACT:</b> Low	<b>\$310.2 billion</b> Rated debt
--	--	--------------------------------------

The higher education sector's vulnerability to cyberattacks derives from its collection and use of sensitive information – ranging from students' personal data to medical records, intellectual property derived from research projects and, in some cases, classified government information in connection with research activities. Further, universities can have tens or even hundreds of thousands of students, and they often engage with entities in multiple geographic locations, exposing their networks to countless access points. Reputational damage could result in declines in enrollment, staff or research funding, while systems disruption would be most acute at research-intensive institutions with academic medical centers.

This sector also includes US not-for-profit entities, primarily cultural and service organizations, foundations and research institutes. Research institutes, like many research-intensive universities, retain significant amounts of highly sensitive data and have a higher degree of vulnerability than others in the sector. Other entities in this sector may retain certain amounts of sensitive data specific to donors, and could be sensitive to loss of donor confidence. Most not-for-profits, however, could likely execute their core mission with a technological disruption.

#### Healthcare




##### Pharmaceuticals

 <b>OVERALL</b> Medium	 <b>VULNERABILITY:</b> Medium  <b>IMPACT:</b> Medium	<b>\$692.3 billion</b> Rated debt
--	---	--------------------------------------

The vulnerability risk for pharmaceutical companies is medium because they do not typically store patient data. While certain patent or intellectual property rights may be stolen, it would be highly unlikely for a rival drug to be developed and marketed given the regulatory approval process and government regulation. However, given the high profile nature of the industry and the market significance of some of the largest firms, the sector may be prone to cyber-attacks that are focused on causing disruption to their business processes. For example, Merck & Co., Inc. experienced a cyberattack in 2017 that reduced its revenue by about \$460 million and caused \$285 million of remediation costs. However, the episode did not significantly affect its brand or reputation.




## Public Infrastructure

## Airports

 <b>OVERALL</b> Medium	 <b>VULNERABILITY:</b> Medium	<b>\$174.3</b> billion
	 <b>IMPACT:</b> Medium	Rated debt

Airports operate essential services but have a limited level of digitization and automation. The primary risk for airports is an attack on one of its many business partners – airlines, air traffic control or passenger security processing – which could disrupt passenger traffic. Our assessment of airports' exposure to cyber risk is focused on direct attacks on airport operations. While they are high-visibility targets, air traffic control facilities are highly redundant and subject to close scrutiny from government cyber security resources, offsetting their susceptibility to attack. Attacks on airline partners are risks covered under the Transportation Services section of this report and the diversity of airline operators at most airports offsets the impact of successful attacks of those entities. Typically, airports do not have access to passengers' personal data. A cyberattack would not likely require physical replacement of assets, but there would be an impact on traffic resulting from flight disruptions. Air travel demand has been resilient in the wake of terrorism, infectious disease and air disasters. Therefore, the impact on airports, and particularly those in the US with full residual cost recovery rate structures, would not likely be extensive.

## Ports

 <b>OVERALL</b> Medium	 <b>VULNERABILITY:</b> Medium	<b>\$27.9</b> billion
	 <b>IMPACT:</b> Medium	Rated debt

Ports operate essential services and have a relatively moderate but increasing level of digitization and automation. Vulnerability will vary. For example, larger ports that serve a populated area are bigger targets than smaller ports. Large, privately managed ports that serve populated areas would typically have a medium-to-high public profile and manage essential assets for the economy in which they operate. In such cases, a cyberattack that disrupts port services for an extended period could have significant repercussions for the service area. The greatest risk is an attack on associated business partners such as shipping lines, cruise lines and processing or inspection facilities. A cyberattack would not likely require physical replacement of assets. However, there would be an impact on volume throughput and port revenue. An information breach could also hurt a port's reputation, weaken its market position and expose it to litigation risk.

## Mass Transit

 <b>OVERALL</b> Medium	 <b>VULNERABILITY:</b> Medium	<b>\$57.5</b> billion
	 <b>IMPACT:</b> Medium	Rated debt

The mass transit sector is exposed to cyber threats because of the potential for high-profile service disruption and the increasing use of computer-based systems to control communications and system operations. The sector includes large rail and subway systems that provide essential commuter services for vast urban areas, which increases their dependence on technology and their exposure to publicity following service interruptions. A temporary loss of customers or an inability to collect fares could have a negative effect on a mass transit system's finances. In addition, recovery costs to restore or repair a system's assets could be somewhat high, depending on the nature of the attack. However, mass transit systems benefit from federal, state and local government funding that provides operating stability and potential support for capital needs. Relatively small bus operators, typically in suburban areas, are less vulnerable to cyber risks because of their minimal digitization, small revenue base and low public profiles.

## Water and Wastewater Utilities

**OVERALL**  
Medium**VULNERABILITY:** Medium**IMPACT:** Medium**\$374.7** billion  
Rated debt




Water and sewer utilities operate critical infrastructure, providing essential services to the broader economy and population. Physical assets are typically run independently, with no internet access and overall limited digital access points for external parties to critical infrastructure. A cyberattack would not likely have a material effect on the actual operation of critical infrastructure assets, but if that did occur it could result in severe disruption. A key strength for both independent regulated utilities and US public finance water and sewer utilities is their monopoly positions. For regulated utilities, regulators would consider the maintenance of service as a key priority and typically allow efficiently incurred costs. Negligent behavior leading to a cyberattack could, however, attract penalties or fines. US public finance water and sewer utilities would generally not incur such penalties. The impact on critical operations will likely differ between individual issuers, depending on backup measures.

## Appendix IV: Summary of medium-low risk sectors

The rate of digitization in these sectors is generally lower compared with higher-risk sectors. Where data is necessary for business processes, medium-low risk sectors are generally able to function with manual workarounds and may benefit from some regulatory protections.




### Governments

#### Sovereign

	<b>OVERALL</b> Medium-Low	 <b>VULNERABILITY:</b> Medium	\$35,778.5 billion Rated debt
		 <b>IMPACT:</b> Low	

The risk of cyberattacks that seek to disrupt government services, access sensitive information or steal resources is an ongoing concern for sovereigns. Most sovereigns have access to highly sensitive personal information, a large revenue base, and sensitive national intelligence information, which increases their vulnerability to attacks. The government's central role in payment and clearing systems, typically through the central bank, also increases vulnerability. The expansion of e-government services, particularly as more citizens gain internet access, also raises vulnerability. However, sovereigns also have strong defense capabilities to protect data and resources, which contain their overall vulnerability to cyberattacks. The impact of a cybersecurity event on a typical sovereign is low. Although sovereigns are high-profile targets, their large scale and diversified economic structure mitigate any material risk to their credit quality. Additionally, past breaches of personal information have had only limited reputational impacts on sovereigns.

#### Regional & Local Governments

	<b>OVERALL</b> Medium-Low	 <b>VULNERABILITY:</b> Medium	\$3,008.4 billion Rated debt
		 <b>IMPACT:</b> Low	

Subsovereign regional and local governments (RLGs) have increasingly turned to digitizing their services for cost and service efficiency, which has increased their exposure to cyberattacks. Regions, provinces, large local governments and capital cities will retain more sensitive personal and business-related data, such as bank account information, credit card information and other personal data for its citizens, than will smaller local governments. This is because sophisticated online payment portals and website traffic help support larger populations and higher volumes of business activity. Access to such data, along with sizable revenue bases and often more liquidity, make larger RLGs more attractive to hackers.

Additionally, larger RLGs are typically responsible for delivering healthcare services and therefore will retain sensitive personal information that hackers may value. Typically, larger RLGs are more likely to be able to fund specific IT programs and withstand an attack financially. Smaller local governments may find it difficult to provide the investment; however, they also face a smaller likelihood of cyberattacks for data extraction. Additionally, smaller RLGs tend to have less money to pay against any ransoming of data, further lowering their potential as targets.




RLGs tend to benefit from strong ties with the central government, which can provide support if necessary. RLGs are also likely to continue to offer many services in the aftermath of a cyberattack. A breach is not likely to severely affect an RLG's brand or result in residents or companies leaving the area. There is moderate risk of a large government facing legal action from taxpayers following a breach or an attack. RLGs generally have strong reserve and liquidity positions, as well as strong market access, to mitigate any financial impact.

US states are vulnerable to cyber threats because of their large revenue base, high public profile and increasing dependence on technology to provide key services. In addition, states collect and are responsible for accurately maintaining a range of highly sensitive, private data for Medicaid recipients, social service recipients and taxpayers. While long-term data loss or corruption could be detrimental to state operations, many state agencies would have the functionality to continue operations over the medium term.

US states are unlikely to incur a materially negative impact from a cyberattack. At the same time, a state has some risk of reputational and financial damage from a cyber event. A significant loss of voter and taxpayer confidence could result in reduced political support and somewhat lower governance predictability. In addition, an attack could temporarily interrupt tax collection and incur capital costs to restore and replace damaged systems. However, the overall impact would be limited by states' substantial available resources, legal protections provided by sovereign immunity and strong cybersecurity governance.

## Education




### School Districts

	OVERALL Medium-Low		VULNERABILITY: Medium	\$41.1 billion Rated debt
			IMPACT: Low	

A severe data breach could expose personal data about students and their families, academic and behavioral history, pertinent medical information and other records. School districts often lack technical staff, key software or active monitoring and preventive measures to secure email and data systems, heightening vulnerability to attacks. A significant cybersecurity breach could affect enrollment and hiring at a school district, particularly because residents have a degree of flexibility in choosing where to work and send a child to school.

## Nonfinancial Corporates

### Consumer Products

 <b>OVERALL</b> Medium-Low	 <b>VULNERABILITY:</b> Medium	\$1,089.4 billion Rated debt
 <b>IMPACT:</b> Low		

As large consumer products and beverage companies with strong brand names and consumer awareness try to leverage social media to promote sales or expand direct online sales, their attractiveness as hacking targets will increase. As with manufacturing companies, any interruption of their supply chain or operations, or damage to products can result in reputational impairment. However, the financial impact of an attack would be relatively low with limited revenue loss because these companies would likely be able to pivot supplier, production and marketing activities to unaffected parties and locations.

### Oil & Gas

OVERALL

Medium-Low

VULNERABILITY: Low

IMPACT: Medium

\$1,694.0 billion




Rated debt

Some subsectors could have somewhat high exposure to cyber risk, but the overall sector has low vulnerability. Exploration and production (E&P) companies distribute their product over numerous production sites and wells, rendering them on the lower end of the risk spectrum for a coordinated attack. Oil & gas producing wells and their control systems rely on electronic networks to some extent, but a widespread disruption of producing wells is not likely. E&P companies maintain large amounts of data, but most of it is not mission critical.

The midstream subsector is more critical to a potential cyberattack because its control systems rely on electronic networks. Disruption caused by a hack into these systems could result in significant supply disruption. Refiners also could have exposure to cyberattacks, but the distributed nature of refineries makes a coordinated attack difficult. In the worst-case scenario, a cyberattack on a refinery's control system could precipitate a severe event such as an explosion or gas leak. Such an event could also result in a refinery going offline temporarily or permanently. An isolated attack on a refinery with significant scale would disrupt the supply of refined products, a scenario that is comparable to shutdowns in the aftermath of hurricanes.

## Housing

### Public Sector Housing

 <b>OVERALL</b> Medium-Low	 <b>VULNERABILITY:</b> Medium	\$155.2 billion Rated debt
 <b>IMPACT:</b> Low		




While social housing providers and housing finance agencies maintain databases of personal information for large numbers of individuals, which can attract attacks, they have a generally low public profile that helps mitigate this risk to some degree. Subsovereign social housing providers receive a significant portion of their revenue from the state, either through transfers or social rents. A cyberattack that affects these transfers or other payment channels could hurt financial performance. For US housing finance agencies, which are tasked with expanding availability of affordable housing by offering below-market-rate mortgages and down payment



assistance to borrowers, an event that results in data loss or corruption would be disruptive to operations until the data could be restored, but, as with social housing providers, it would likely have limited impact on the agency's reputation.

## Structured Finance

### Structured Finance

 <b>OVERALL</b> Medium-Low	 <b>VULNERABILITY:</b> Medium	\$4,817.0 billion Rated debt
 <b>IMPACT:</b> Low		




The nature of structured finance transactions, in which the sponsor and the structured transaction are legally separate, mitigates the transfer of any risk to the transaction itself. The reputational damage that could stem from a large and public data breach of a transaction sponsor would likely have little effect on the payments of the obligors of an existing transaction. An attack that is severe enough to disrupt the operations of a sponsor that also services the loans or an independent third-party servicer or trustee could temporarily disrupt transaction cash flow. However, the likelihood is small that such a disruption would last long enough to have a significant credit impact on the structured transaction.

## Appendix V: Summary of low-risk sectors

These sectors have a relatively low reliance on technology and on data to maintain business operations, and they often have well-established manual workarounds. Many low-risk sectors also benefit from strong regulatory protections that allow them to operate with a monopoly-like market position or they can offset losses through pricing adjustments (for example, through tax revenue). These sectors have little or no emerging trends that will alter their cyber risk profiles in the next few years.




### Nonfinancial Corporates

#### Basic Commodities

 OVERALL Low	 VULNERABILITY: Low  IMPACT: Low	\$930.3 billion Rated debt
--	---	-------------------------------

These industries have low risk given the fragmented nature of their operations, with plants, mines and facilities in multiple locations and geographies. The businesses have decentralized operations, which limits the extent of damage from a cyberattack on any given site. The lack of consumer awareness of the companies supplying the product or service also makes these industries less desirable for cyber criminals than more highly visible and recognizable sectors.




#### Real Estate

 OVERALL Low	 VULNERABILITY: Low  IMPACT: Low	\$656.9 billion Rated debt
--	---	-------------------------------

These industries have distributed operations and assets, which will limit the extent of damage from a cyberattack on any given revenue center. The lack of consumer awareness of the companies supplying the product or service also makes these industries less desirable for cyber criminals than more highly visible and recognizable sectors.

### Public Infrastructure




#### Toll Roads

 OVERALL Low	 VULNERABILITY: Low  IMPACT: Low	\$217.3 billion Rated debt
--	---	-------------------------------

In the event of a cyberattack, toll roads would likely still be able to remain open to traffic. Business interruption would be minimal. An attack could have a larger effect on revenue collection, however, depending on the collection system in use (free-flow with automated plates recognition versus standard traffic barriers). Most rated issuers in the sector collect revenue through toll barriers with a few notable exceptions. Unintended data disclosure could expose a toll road to litigation risk, but the risk is lower compared with that of other sectors. Single-asset project finance issuers with a shadow-toll tariff structure, in which the toll road is free to users as payments are received from the government based on traffic, have less exposure than networks or single-asset project financings with user-paid tolls. The impact of a cyberattack would be localized.

### Public Private Partnerships

#### PPP

 OVERALL Low	 VULNERABILITY: Low  IMPACT: Low	\$41.3 billion Rated debt
--	---	------------------------------

The diverse array of assets that can be procured and financed using the PPP model, including hospitals, government buildings, roads and bridges, does not lend itself perfectly to scoring the sector as a whole. However, most PPPs have common characteristics. For example, nearly all of them (1) are single assets, which increases the impact of an asset shutdown or interruption; (2) use a computerized system to track performance, which can affect annual revenue; (3) encompass low-profile assets such as toll roads, although some are high profile including government assets related to national security, large-scale regional hospitals or essential commuter rail lines; (4) are owned and operated by an unknown operator or sponsor; and (5) can be politicized when issues occur. The

type of data and information collected tends to be more limited compared with commercial and government systems, which generally house more sensitive and valuable user information.

DRAFT-CONFIDENTIAL

## Moody's related publications

### Sector research

- » [Insurance - Global: \(Re\)Insurers step up tech investment as disruption threat grows](#), November 14, 2018
- » [Regulated electric and gas utilities - US: Cyber risk is on the rise, but the likelihood of government relief is high](#), September 17, 2018
- » [Banking: Chile issues new cybersecurity regulations, a credit positive for banks](#), September 3 2018
- » [Local government – Washington: Washington State cybersecurity audits help mitigate risk from growing threat](#), August 14, 2018
- » [Banking: Data-sharing partnerships between technology-enabled firms and big US banks would be credit negative for regional banks](#), August 8, 2018
- » [Banks: Russian central bank's additional capital requirement for banks' cyber risks would be credit positive](#), February 26, 2018
- » [Public power electric utilities - US: Growing grid interconnectivity increases cybersecurity risks](#), June 16, 2017
- » [Asset Managers - US managers sharpen their focus on cybersecurity](#), June 1, 2017
- » [Banks - US: Cybersecurity will improve under new requirements of New York regulator](#), February 23, 2017
- » [Insurers - US and Canada: Survey: North American Insurers Step up Cybersecurity Initiatives](#), February 13, 2017
- » [Utilities Remain Vulnerable and Attractive Target of Cyber Attacks, a Credit Negative](#), January 9, 2017

### Issuer research

- » [Marriott announces credit-negative data security incident](#), November 30, 2018
- » [Equifax: Updated credit analysis](#), October 31, 2018
- » [Tesco Bank fined £16.4 million for 2016 cyberattack, a credit negative](#), October 8, 2018
- » [Envigo Laboratories Inc.: Update to credit analysis following downgrade of CFR to Caa2](#), September 28, 2018
- » [BMO and CIBC suffer a credit-negative customer data privacy breach](#), June 4, 2018
- » [Equifax: Continuing fallout from cybersecurity breach will erode profitability in 2018 and litigation risks will remain high](#), March 5, 2018
- » [FedEx Corporation: Update to credit analysis - Expected deleveraging remains on track](#), September 28, 2017
- » [Equifax's security breach is credit negative but Baa1 rating unaffected](#), September 8, 2017
- » [Merck & Co.: Credit negative cyber-attack is mitigated by positive business fundamentals](#), July 28, 2017

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

- <sup>1</sup> See [The untold story of NotPetya, the Most Devastating Cyberattack in History](#), Wired, August 22, 2018.
- <sup>2</sup> The electric utilities category includes issuers rated under the following methodologies: regulated electric and gas networks, unregulated utilities and unregulated power companies, regulated electric and gas utilities, public power utilities and power generation.
- <sup>3</sup> See [Corporate cash pile declines 9.5% to \\$1.8 trillion; tech extends lead over other sectors](#), November 27, 2018.

© 2019 Moody's Corporation, Moody's Investors Service, Inc., Moody's Analytics, Inc. and/or their licensors and affiliates (collectively, "MOODY'S"). All rights reserved.

CREDIT RATINGS ISSUED BY MOODY'S INVESTORS SERVICE, INC. AND ITS RATINGS AFFILIATES ("MIS") ARE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MOODY'S PUBLICATIONS MAY INCLUDE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES. MOODY'S DEFINES CREDIT RISK AS THE RISK THAT AN ENTITY MAY NOT MEET ITS CONTRACTUAL FINANCIAL OBLIGATIONS AS THEY COME DUE AND ANY ESTIMATED FINANCIAL LOSS IN THE EVENT OF DEFAULT OR IMPAIRMENT. SEE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS AND MOODY'S OPINIONS INCLUDED IN MOODY'S PUBLICATIONS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S PUBLICATIONS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. CREDIT RATINGS AND MOODY'S PUBLICATIONS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. NEITHER CREDIT RATINGS NOR MOODY'S PUBLICATIONS COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS AND PUBLISHES MOODY'S PUBLICATIONS WITH THE EXPECTATION AND UNDERSTANDING THAT EACH INVESTOR WILL, WITH DUE CARE, MAKE ITS OWN STUDY AND EVALUATION OF EACH SECURITY THAT IS UNDER CONSIDERATION FOR PURCHASE, HOLDING, OR SALE.

MOODY'S CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS OR MOODY'S PUBLICATIONS WHEN MAKING AN INVESTMENT DECISION. IF IN DOUBT YOU SHOULD CONTACT YOUR FINANCIAL OR OTHER PROFESSIONAL ADVISER. ALL INFORMATION CONTAINED HEREIN IS PROTECTED BY LAW, INCLUDING BUT NOT LIMITED TO, COPYRIGHT LAW, AND NONE OF SUCH INFORMATION MAY BE COPIED OR OTHERWISE REPRODUCED, REPACKAGED, FURTHER TRANSMITTED, TRANSFERRED, DISSEMINATED, REDISTRIBUTED OR RESOLD, OR STORED FOR SUBSEQUENT USE FOR ANY SUCH PURPOSE, IN WHOLE OR IN PART, IN ANY FORM OR MANNER OR BY ANY MEANS WHATSOEVER, BY ANY PERSON WITHOUT MOODY'S PRIOR WRITTEN CONSENT.

CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT INTENDED FOR USE BY ANY PERSON AS A BENCHMARK AS THAT TERM IS DEFINED FOR REGULATORY PURPOSES AND MUST NOT BE USED IN ANY WAY THAT COULD RESULT IN THEM BEING CONSIDERED A BENCHMARK.

All information contained herein is obtained by MOODY'S from sources believed by it to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, all information contained herein is provided "AS IS" without warranty of any kind. MOODY'S adopts all necessary measures so that the information it uses in assigning a credit rating is of sufficient quality and from sources MOODY'S considers to be reliable including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the rating process or in preparing the Moody's publications.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY CREDIT RATING OR OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby discloses that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any rating, agreed to pay to Moody's Investors Service, Inc. for ratings opinions and services rendered by it fees ranging from \$1,000 to approximately \$2,700,000. MCO and MIS also maintain policies and procedures to address the independence of MIS's ratings and rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold ratings from MIS and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at [www.moody's.com](http://www.moody's.com) under the heading "Investor Relations — Corporate Governance — Director and Shareholder Affiliation Policy."

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited ABN 61 003 399 657 AFSL 336969 and/or Moody's Analytics Australia Pty Ltd ABN 94 105 136 972 AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761G of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761G of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not on the equity securities of the issuer or any form of security that is available to retail investors.

Additional terms for Japan only: Moody's Japan K.K. ("MJKK") is a wholly-owned credit rating agency subsidiary of Moody's Group Japan G.K., which is wholly-owned by Moody's Overseas Holdings Inc., a wholly-owned subsidiary of MCO. Moody's SF Japan K.K. ("MSFJ") is a wholly-owned credit rating agency subsidiary of MJKK. MSFJ is not a Nationally Recognized Statistical Rating Organization ("NRSRO"). Therefore, credit ratings assigned by MSFJ are Non-NRSRO Credit Ratings. Non-NRSRO Credit Ratings are assigned by an entity that is not a NRSRO and, consequently, the rated obligation will not qualify for certain types of treatment under U.S. laws. MJKK and MSFJ are credit rating agencies registered with the Japan Financial Services Agency and their registration numbers are FSA Commissioner (Ratings) No. 2 and 3 respectively.

MJKK or MSFJ (as applicable) hereby disclose that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by MJKK or MSFJ (as applicable) have, prior to assignment of any rating, agreed to pay to MJKK or MSFJ (as applicable) for ratings opinions and services rendered by it fees ranging from JPY125,000 to approximately JPY250,000,000.

MJKK and MSFJ also maintain policies and procedures to address Japanese regulatory requirements.

REPORT NUMBER

1145309



## Contacts

**Jim Hempstead** +1.212.553.4318  
*MD-Utilities*  
 james.hempstead@moody's.com

**Sebastien Hay** +34.91.768.8222  
*Senior Vice President/  
 Manager*  
 sebastien.hay@moody's.com

**Lina Choi** +852.3758.1369  
*VP-Sr Credit Officer*  
 lina.choi@moody's.com

**Baye Larsen** +1.212.553.0818  
*VP-Sr Credit Officer*  
 baye.larsen@moody's.com

**Michael Osborn** +1.212.553.7799  
*VP-Senior Analyst*  
 michael.osborn@moody's.com

**Philip Cope** +44.20.7772.5229  
*AVP-Analyst*  
 philip.cope@moody's.com

**David Rogovic** +1.212.553.4196  
*AVP-Analyst*  
 david.rogovic@moody's.com

**Sarah Hibler** +1.212.553.4912  
*Associate Managing  
 Director*  
 sarah.hibler@moody's.com

**Frank Cervený** +49.69.70730.730  
*VP-Senior Research  
 Analyst*  
 frank.cervený@moody's.com

**William Foster** +1.212.553.4741  
*VP-Sr Credit Officer*  
 william.foster@moody's.com

**Peter McNally** +1.212.553.3610  
*VP-Senior Analyst*  
 peter.mcnally@moody's.com

**Abhishek Tyagi** +65.6398.8309  
*VP-Senior Analyst*  
 abhishek.tyagi@moody's.com

**Lesley Ritter** +1.212.553.1607  
*AVP-Analyst*  
 lesley.ritter@moody's.com

**Jennifer Zong** +1.212.553.0110  
*Associate Analyst/CSR*  
 jennifer.zong@moody's.com

## CLIENT SERVICES

**Americas** 1-212-553-1653

**Asia Pacific** 852-3551-3077

**Japan** 81-3-5408-4100

**EMEA** 44-20-7772-5454