MOODY'S
INVESTORS SERVICE

SECTOR IN-DEPTH
2 October 2019

Rate this Research

TABLE OF CONTENTS

Contacts

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

Brendan Sheehan +1.212.553.0402
VP-Senior Analyst
brendan.sheehan@moodys.com

Poonam Thakur +1.212.553.4635
Associate Analyst
poonam.thakur@moodys.com

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

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

Cyber Risk – Global

Cyber disclosures reveal varying levels of transparency across high-risk sectors

» **Corporate cyber risk disclosures provide contrasting levels of transparency.** Corporate disclosures regarding cyber risk vary greatly across the sectors we identify as having elevated cybersecurity risk. As cyberattacks increase in frequency, a lack of transparency about cybersecurity strategies could erode investor confidence and affect credit quality.

» **Banks, telecommunications & media companies provide the most detailed disclosures among the sectors analyzed**. They go beyond citing cyber risk and their board oversight practices, and discuss in fairly specific terms their cybersecurity risk management strategies.

» **Hospitals and other healthcare providers have the least complete disclosures among the four sectors most at risk of a cyberattack.** Although all 10 of the companies we examined in this sector highlight cyber risk as a growing threat in their disclosures, fewer than half detail how their board oversees cyber risk, while only a handful discuss their strategy for managing the risk.

» **Market infrastructure providers, securities firms and electric utilities provide above-average disclosures.** Nearly all the companies in these sectors list cybersecurity as a risk and discuss some level of governance on the issue. Most of these companies also list cyber insurance as a mitigant to the financial exposure associated with cyber risk.

» **Sectors with the most limited disclosures include retail, lodging, health insurance, medical devices and transportation services.** In these sectors, the companies' risk discussions do not consistency cite cybersecurity. Also, they have less-robust disclosures around the governance structure of this risk, and few of them provide details about cyber risk mitigation.

» **US and European companies are more transparent than their Asian peers.** While nearly all companies mention cybersecurity risk, US-based companies appear more reliant on cyber insurance as a means to manage the risk, while their European counterparts are more likely to offer a detailed discussion about their strategy to mitigate the operational impact of a cyberattack.

» **Investment-grade companies provide more detail about their cybersecurity measures.** Investment-grade companies typically have greater financial resources to draw on and are more likely to have the internal staffing and infrastructure to generate cybersecurity disclosures.

Corporate cyber risk disclosures provide contrasting levels of detail and transparency

The level of detail that companies share about how they oversee and manage cybersecurity risk varies greatly by sector and region, according to our review of 2018 annual financial statements and 2019 proxy statements (or equivalent) of companies operating in sectors with elevated cybersecurity risk. Our analysis is based on public disclosures from 125 companies in North America, EMEA and Asia. These companies comprise the largest rated debt issuers in each of the sectors we have identified as having high or medium-high cybersecurity risk. (See appendices for our definitions of cyber risk levels, a breakdown of cyber risk exposure by sector, and a list of the companies whose disclosures we analyzed.)

Cyber disclosures deemed most relevant to our analysis fall into three broad categories: risk factor discussion, board-level oversight, and risk management. Elements of disclosure that we specifically looked for within those categories are defined in Exhibit 1. An average disclosure in our sample group contains some discussion of the elements in the first two categories, meaning that it addresses the cybersecurity risk facing the enterprise and describes the board governance structure assigned to oversee the risk. Below-average disclosure fails consistently to address even the first two categories, while stronger disclosures go further and detail a company's approach to managing this risk.

Exhibit 1

What we consider when judging the breadth of cybersecurity disclosures

Three cybersecurity disclosure categories broken down by subcategory

Categories		Subcategories	Why it matters?
1.	**Risk Discussion**	1. Operational, reputational, regulatory, and financial risks specific to the company such as: data security, critical physical infrastructure, third-party cyber risk, exposure to data privacy laws.	Recognizing the rapid pace of digitization across industries and the growing number of cyber attacks being reported, calling out cyber risk as an operational, reputational, and financial risk should be common practice by now. But merely referencing it as a risk is insufficient. The stronger disclosures acknowledge cyber as an enterprise-wide issue and describe the relevant nuances cyber risk poses to the company.
2.	**Risk Oversight**	1. Board committee responsible for cyber risk oversight 2. Board members with cyber experience and/or training 3. Chief information security officer (CISO) or equivalent, reporting frequency to Board	Information about a company's cyber risk oversight will offer insight into its attention to this risk and the internal expertise it has to call upon to help manage this risk.
3.	**Risk Management**	1. Access to cyber insurance 2. Board approved global cybersecurity strategy 3. Risk management strategy including: embedded security personnel across business lines, reporting structure between CISO or equivalent and executive team, presence of 24/7 global emergency response team, etc.	Participants in each sector has experienced a cyber attack and companies recognize that they cannot guarantee they will not be attacked in the future. Cyber risk management is therefore critical since it mitigates the risk by seeking to minimize the number of attacks and improve the recovery prospects from an attack.

Source: Moody's Investors Service

The level of transparency of a company's cybersecurity disclosures does not necessarily reflect the degree to which the company is prepared to deal with such threats. Some companies choose to withhold information about their cyber defense strategies for security reasons. Others may fear that being cited as a cybersecurity leader would only encourage attacks. Still, sharing details about, say, board-level oversight procedures can demonstrate a basic level of maturity in how a company manages its exposure to cyber threats without providing the type of information that is likely to draw the attention of attackers.

From a credit perspective, disclosure is less important than actual defense in depth measures and an impactful mitigation strategy. That said, cybersecurity public disclosures are a useful tool to compare and contrast how companies in sectors with elevated risk are addressing these challenges.

For example, confidence sensitive sectors, such as financial institutions, rely on investors and thus provide detailed disclosures of cyber risk mitigation and oversight. The absence of more detailed disclosures can make it difficult to assess a company's preparedness to

manage cyber risk. As successful cyberattacks increase in frequency, a lack of transparency could ultimately erode investor confidence and complicate efforts by companies to raise capital and access liquidity.

Regulators are paying close attention to the issue, as was evident in the US Securities and Exchange Commission's (SEC) February 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, which sought to promote the timely and accurate disclosure of cybersecurity risks and incidents. The SEC recommended that companies address cyber risk in similar levels of detail as they do economic and business risk, particularly as it relates to internal controls, financial reporting and timely public disclosures.

The commission's guidance seeks to move cyber disclosures in a more prescriptive direction that will, over time, generate more consistent and reliable information. The SEC's previous cyber guidance relied heavily on the subjective judgment of corporate counsel to determine what to disclose. As a result, information on cyber events was inconsistent. The SEC's Investor Advisory Committee observed in its December 2017 Discussion Draft Re: Cybersecurity and Risk Disclosure that public company disclosures regarding cybersecurity incidents had not meaningfully improved since 2011. Furthermore, an SEC review of 2017 breach data found that only four of the 82 cybersecurity incidents at public companies in 2017 were followed by the filing of an 8-K disclosing the breach to investors.

Banks, telecommunications and media provide the most detailed disclosures

Banks and telecommunications & media companies disclose the most information about their cybersecurity measures among the sectors that we have identified as having significant exposure to cyber risk. Companies in these sectors consistently go beyond the baseline disclosure that recognizes cybersecurity as a growing enterprise risk and describes their oversight of cybersecurity risk. About half of the companies offer a detailed account of their risk management strategy and mention the company's adoption of a board-approved global cybersecurity strategy. Cybersecurity disclosures in the banking and telecom & media sectors also appear to meet the disclosure controls and procedures recommendations in the SEC's 2018 cybersecurity guidance.

Exhibit 2

Banks and telecom & media companies provide the most information

Number of companies in sectors with high/medium-high cyber risk that provide disclosure in each subcategory

			Risk Discussion	Risk Oversight			Risk Management			
Sector	Total # of Issuers	Cyber Risk	Management Discussion & Analysis	Board Committee	Director Qualifications	CISO interaction with Board	Cyber Insurance	Detailed Risk Mitigation Strategy	Global Cyber Strategy	# of Above Average Subcategories
Banks	10	High	10	7	5	5	3	5	5	7
Telecommunications & Media	10	Med-High	10	4	3	3	5	5	2	6
Securities Firms and Market Infrastructure Providers	18	High	17	9	7	2	8	9	4	5
Electric Utilities	10	Med-High	8	3	6	2	4	3	3	5
Lodging, Gaming & Cruise	10	Med-High	10	7	2	0	7	1	0	3
Retail	10	Med-High	7	7	3	2	1	0	0	3
Technology	10	Med-High	8	6	3	2	1	2	0	3
Health Insurance	7	Med-High	7	6	2	0	0	0	0	2
Medical Devices	10	Med-High	9	5	1	2	1	1	1	2
Hospitals and Healthcare Providers	10	High	10	4	1	0	2	1	1	1
Manufacturing & Auto	10	Med-High	7	3	2	0	1	3	0	1
Transportation Services	10	Med-High	8	6	2	0	1	2	1	1

Blue shading indicates tallies that exceed the average for the subcategory across all analyzed sectors.
Sources: Company public disclosures and Moody's Investors Service

The banking sector is one of four sectors we have classified as being most at risk of experiencing a material cyberattack. Banks with the most transparent and complete cybersecurity disclosures include JPMorgan Chase & Co. (A2 stable), BNP Paribas (Aa3 stable), Société Générale (A1 stable), and Citigroup Inc. (A3 stable). In addition to the baseline disclosure about cyber risk and oversight that we were looking for, they offer substantial details about their respective risk management strategy. Their disclosures include details about the structure and reporting lines of their cybersecurity team; address the partnership between the cybersecurity team and the company's lines of business, including the presence of embedded cybersecurity personnel at the line of business level; and mention the existence of a 24/7, global cyber emergency response team. Some, like Société Générale (A1 stable), even disclose how much capital they invest in their cybersecurity initiatives.

Telecom & media companies are at a medium-high risk of experiencing a material cyberattack according to our cyber risk heat map. Like banks, their cybersecurity disclosures stand out for their level of transparency and detail, especially those of Verizon Communications Inc. (Baa1 positive), Vodafone Group PLC (Baa2 negative) and Sprint Corporation (B2 review for upgrade). However, the two sectors differ somewhat in terms of the number of companies that refer to access to cyber insurance and adoption of a board-approved global risk strategy. Banks highlight the latter more frequently, which could point to a more sophisticated appreciation of cyber risk and a deliberate, proactive approach to managing it. Telecom & media companies appear to be heavier adopters of cyber insurance, which provides a way to transfer financial risk to a third party. But the amount, type or scope of coverage are typically not disclosed.

Cyber insurance coverage program limits of $25 million to $100 million are now common, with some companies able to purchase as much as $750 million in coverage (see "P&C Insurance — Global: Battling hidden cyber exposures, insurers position for growing opportunity"). However the cost of recovering from an attack can reach into the hundreds of millions dollars, as FedEx Corporation (Baa2 stable) demonstrated when it reported $400 million in costs associated with the NotPetya cyberattack during fiscal 2018. Furthermore, coverage of fines and regulatory penalties resulting from a cyberattack is unclear. In most jurisdictions, insurers are legally prohibited from indemnifying fines and regulatory penalties because doing so may undermine the intention of the law. As fines grow, sometimes even exceeding $100 million, the financial impact can be significant.

Hospitals and other healthcare providers have the least detailed disclosures among the sectors most at risk of a cyberattack

Hospitals and other healthcare providers are less transparent about their cyber risk oversight and management strategies than other high-risk sectors. Despite consistently acknowledging that cyber threats pose a material risk to their operations, reputation and financial strength, fewer than half provide details about their cybersecurity board oversight structure and only one, Encompass Health Corp. (Ba3 stable), gives any information about the cyber qualifications of its board members. In addition, only two mention access to cyber insurance and one, Fresenius SE & Co. KGaA (Baa3 stable), provides a more in-depth discussion of its cybersecurity risk management strategy.

We think the absence of more detailed disclosures makes it difficult for investors to assess a company's level of preparedness, or engage with company management on their future plans.

Securities firms & market infrastructure providers and electric utilities provide above-average disclosures

Nearly all securities firms, market infrastructure providers and electric utilities in our sample group list cybersecurity as a risk and display some level of oversight over the issue. They detail their company's governance structure, including the board committee in charge of cybersecurity oversight, along with biographies of the board members with cybersecurity expertise. Some, like Nasdaq Inc. (Baa2 stable) and London Stock Exchange Group plc (A3 review for downgrade) even reference a board approved multi-year cybersecurity strategic plan. From a risk management standpoint, about half of these companies list cyber insurance as a partial mitigant to cybersecurity risk and the same percentage of companies offers details about their internal risk management practices.

That said, there are regional differences in the level of disclosure in this group. All three sectors include a number of Asian companies that are generally less transparent in their cyber disclosures and often fail to even address cybersecurity in their risk discussion. Excluding Asian companies, the strength of cybersecurity disclosures at market infrastructure providers & securities firms would be more in-line with that of the banking sector.

There is a further regional distinction between US and European electric utilities. Large European electric integrated utilities like Iberdrola S.A (Baa1 stable), Enel S.p.A. (Baa2 positive) and Electricité de France (A3 stable) provide extensive details about their cyber risk management strategy. By contrast, US utilities in the sector provide more boilerplate disclosures acknowledging cybersecurity risk, their board oversight structure and their access to cyber insurance, with none mentioning the existence of a board-approved global cyber strategy.

Other sectors with medium-high risk provide the most limited disclosures

Lodging, gaming and cruise, health insurance, manufacturing and autos, medical devices retail, technology and transportation services all face medium-high cyber risk, but their cybersecurity disclosures are the most limited in our sample group of companies. Companies

in these sectors did not consistently cite cybersecurity in the risk discussions sections of their financial reports, and disclosures addressing the oversight of this risk are significantly less robust. Furthermore, most disclosures are limited to boilerplate language without addressing the risk nuances relevant to their respective businesses. Moreover, few address risk management in any meaningful way and, apart from lodging, gaming and cruise, only a limited number reference access to cyber insurance.

The lack of detailed disclosures in these sectors is surprising given that retailer Target Corporation (A2 stable), lodging company Marriott International Inc. (Baa2 stable), and transportation services company FedEx all fell victim to highly publicized, large-scale cybersecurity attacks.

Exhibit 3

Limited disclosures in lodging, transportation services and retail despite high-profile attacks

Large-scale cyberattacks on Marriott, FedEx and Target

Issuer	Date	Description
Marriott international Inc.	Nov-18	Breach of Starwood guest reservation database, affecting up to 383 million guest records. Breached data included names, addresses, credit card numbers, phone numbers, passport numbers, travel locations and arrival and departure dates.
FedEx Corporation	Jun-17	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.
Target Corporation	Dec-13	Data breach that exposed the names, mailing, address, phone numbers and email addresses for up to 70 million individuals.

Source: Company information

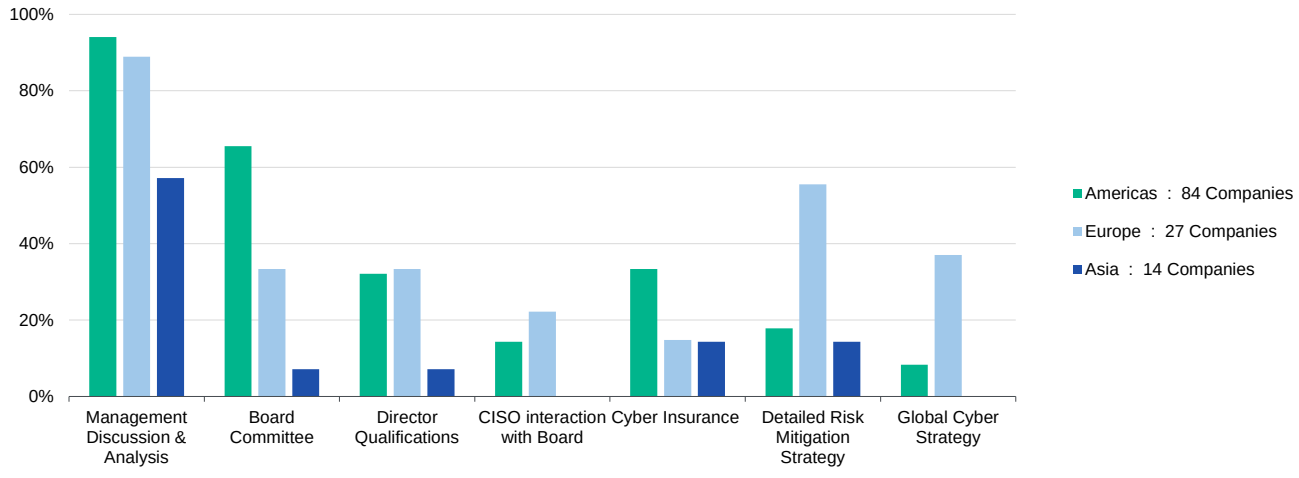
US and European companies are more transparent than their Asian peers

Companies headquartered in the US and Europe tend to have more complete disclosures than those based in the Asia Pacific region. Less than 60% of the Asian companies in our sample group cite cybersecurity in the risk section of their financial disclosures, while 90% of US and European companies mention it (see Exhibit 4). APAC jurisdictions typically have fewer regulatory disclosure requirements regarding corporate governance and board oversight, which may be a reason for the more limited cyber discussion from companies in the region.

Exhibit 4

Disclosures tend to be weaker among Asian companies

Percentage of companies by region that provide key components of cybersecurity disclosure



Sources: Company filings and Moody's Investors Service

However, despite their similar level of attention to citing cybersecurity risk, there is a difference in how companies in the two regions discuss how they manage this risk. US companies appear more reliant on cyber insurance as a mitigant, while their European counterparts are more likely to offer a detailed discussion about their internal infrastructure to manage cyber risk.

This difference in disclosure approach may be a reflection of differing regulatory and cultural regimes in the US and Europe. US companies focus heavily on minimizing the financial impact of potential cyber events, which is emblematic of the shareholder primacy model of most US companies. Shareholder lawsuits against US companies in the wake of cyber breaches and other material events are common and may encourage companies to disclose safeguards to protect investors from potential cyber costs. Additionally, some US companies fear that disclosures detailing preemptive mitigation programs that subsequently fail to prevent cyberattack will expose them to disclosure-focused shareholder objection suits that are commonplace in mergers and acquisition transactions. In Europe, where shareholder litigation is less common, companies may choose to provide greater transparency on steps in place to mitigate the actual occurrence of cyber events.

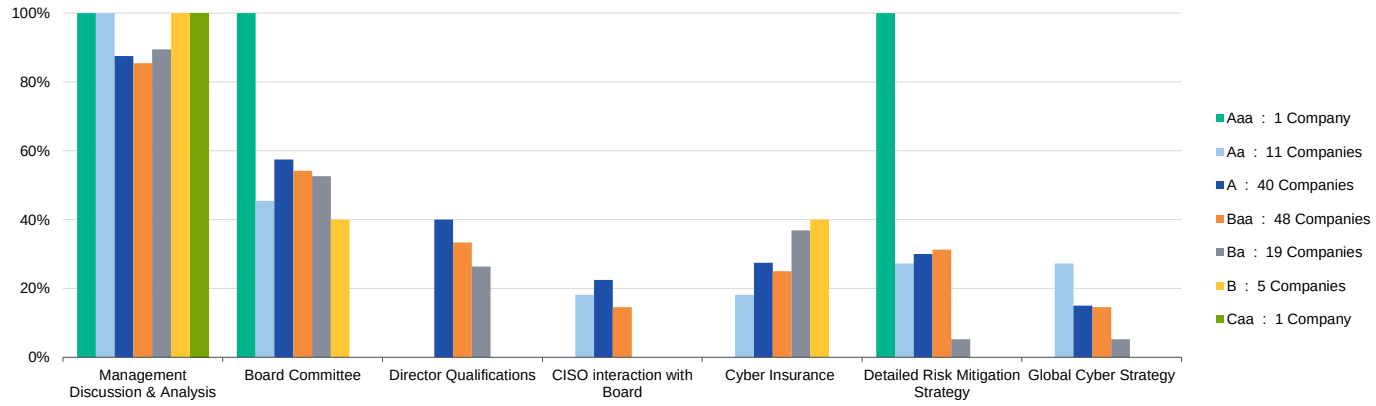
Investment-grade companies provide more detail than do others

The quality and transparency of cyber disclosures are typically more robust for more highly rated companies. About 40% of the investment-grade companies in our sample group provide some discussion about cyber risk management. They are also be more forthcoming in their discussion about board oversight and reporting structure than speculative-grade companies. This is not surprising given that investment-grade companies typically have greater financial resources to draw on and are more likely to have the internal staffing and infrastructure to generate cybersecurity disclosures.

Exhibit 5

Cyber disclosures of investment-grade companies are more transparent than those of their speculative-grade counterparts

Percentage of companies by rating category that provide key components of cybersecurity disclosure



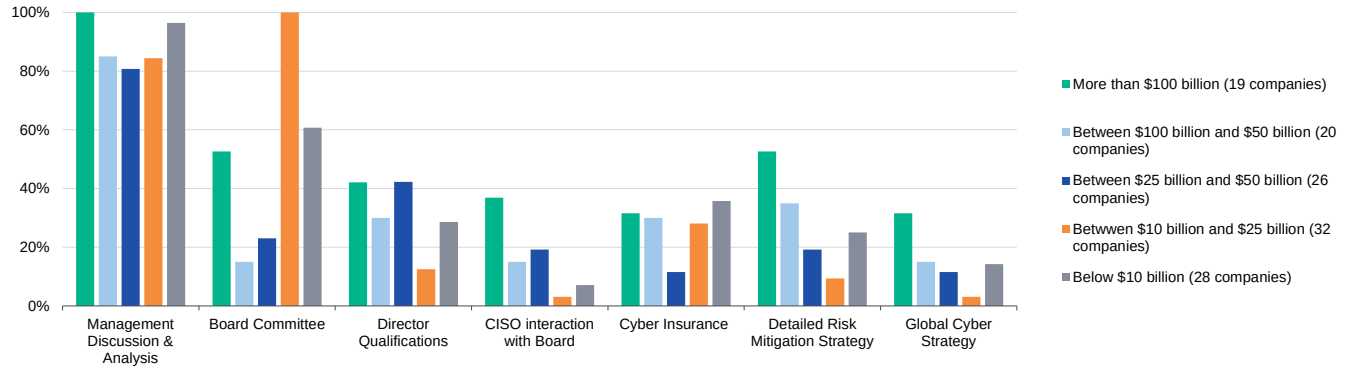
This graph uses senior unsecured ratings for investment-grade companies and corporate family ratings for speculative-grade companies.
Sources: Company filings and Moody's Investors Service

Similarly, larger debt issuers typically provide greater transparency in their cybersecurity disclosures. This, too, is not surprising because the largest debt issuers are typically very sizable companies with significant resources and greater financial flexibility.

Exhibit 6

Cyber disclosures for large debt issuers are more transparent than disclosures cited by smaller counterparts

Percentage of companies by amount of rated debt that provide key components of cybersecurity disclosure



Debt quantum is based on Moody's Adjusted Total Debt as of year-end 2018

Sources: Company filings and Moody's Investors Service

Appendix A

Exhibit 7
How we define levels of cyber risk
Cyber risk assessment levels

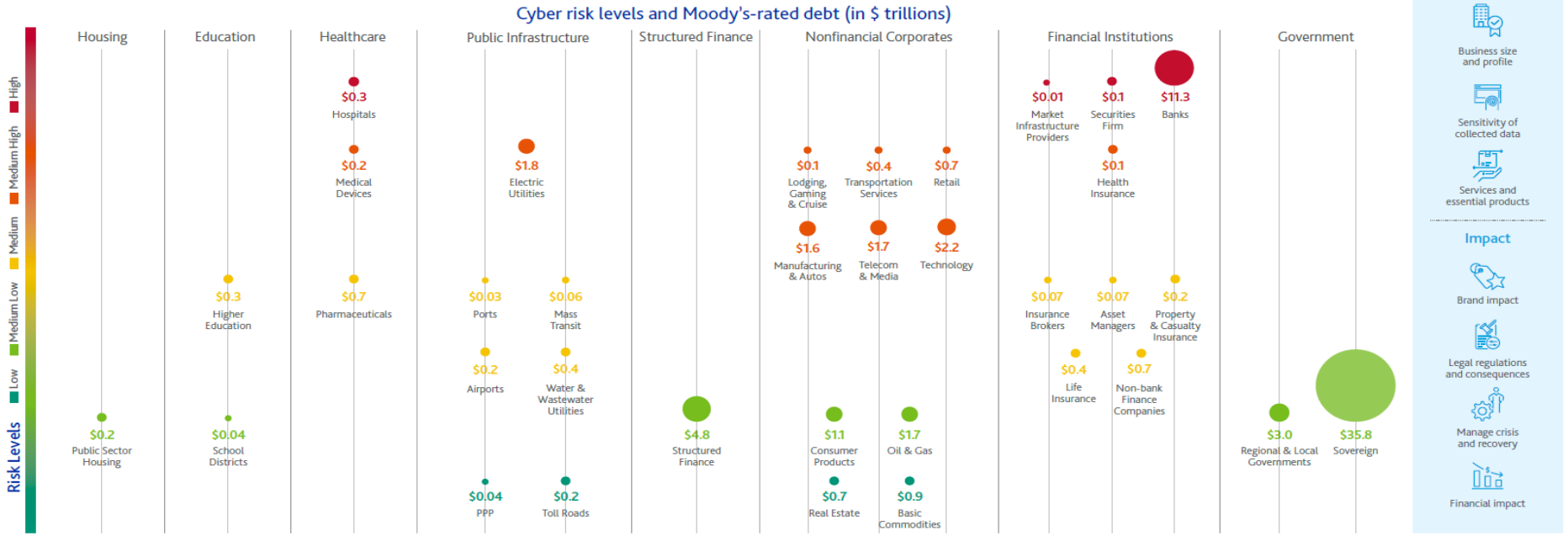
LEVELS	
HIGH	These sectors have a significant reliance on technology and confidential information for their operations and are highly interconnected, both internally and externally. As a result, they will often have a limited ability to fall back on manual operations, either because of the nature of 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).
MEDIUM HIGH	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.
MEDIUM	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.
MEDIUM LOW	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.
LOW	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.

Taken from our February 2019 report, "Cross-Sector – Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects."
Source: Moody's Investors Service

Appendix B

Cyber Risk: Credit Risk Exposure by Sector

The growing intersection of supply chains, connectivity and access to data is increasing the potential for significant cyberattacks, creating new risks for governments and businesses worldwide. Moody's assessed 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.



Source: Moody's Investors Service

Appendix C

Our sample group of 125 companies in sectors with high or medium-high cyber risk

Company	Rating	Sector	Region	Cyber Risk Level	Total Debt ($MM)
Bank of America Corporation	A2	Banks	Americas	High	$ 514,623
BNP Paribas	Aa3	Banks	Europe	High	$ 501,797
Citigroup Inc.	A3	Banks	Americas	High	$ 460,648
Goldman Sachs Group, Inc. (The)	A3	Banks	Americas	High	$ 386,515
JPMorgan Chase & Co.	A2	Banks	Americas	High	$ 580,690
Morgan Stanley	A3	Banks	Americas	High	$ 269,448
Nordea Bank AB	Aa3	Banks	Europe	High	$ 240,559
Rabobank	Aa3	Banks	Europe	High	$ 179,836
Société Générale	A1	Banks	Europe	High	$ 392,237
Westpac Banking Corporation	Aa3	Banks	Asia	High	$ 147,276
CHS/Community Health Systems, Inc.	Caa3	Hospitals and Healthcare Providers	Americas	High	$ 15,108
DaVita Inc.	Ba2	Hospitals and Healthcare Providers	Americas	High	$ 12,955
Encompass Health Corp.	Ba3	Hospitals and Healthcare Providers	Europe	High	$ 2,943
Fresenius Medical Care AG & Co. KGaA	Baa3	Hospitals and Healthcare Providers	Europe	High	$ 15,272
Fresenius SE & Co. KGaA	Baa3	Hospitals and Healthcare Providers	Europe	High	$ 30,642
HCA Healthcare, Inc.	Ba1	Hospitals and Healthcare Providers	Americas	High	$ 35,061
Ramsay Generale de Sante	Ba3	Hospitals and Healthcare Providers	Europe	High	$ 3,977
Select Medical Holdings Corporation	B1	Hospitals and Healthcare Providers	Americas	High	$ 4,595
Tenet Healthcare Corporation	B2	Hospitals and Healthcare Providers	Americas	High	$ 16,516
Universal Health Services, Inc.	Ba1	Hospitals and Healthcare Providers	Americas	High	$ 4,456
Charles Schwab Corporation (The)	A2	Securities Firms and Market Infrastructure Providers	Americas	High	$ 9,005
CITIC Securities Company Limited	Baa1	Securities Firms and Market Infrastructure Providers	Asia	High	$ 44,839
CME Group Inc.	Aa3	Securities Firms and Market Infrastructure Providers	Americas	High	$ 4,882
Daiwa Securities Group Inc.	Baa1	Securities Firms and Market Infrastructure Providers	Asia	High	$ 93,546
E*TRADE Financial Corp.	Baa2	Securities Firms and Market Infrastructure Providers	Americas	High	$ 1,965
Goldman Sachs International	A1	Securities Firms and Market Infrastructure Providers	Americas	High	$ 206,303
Intercontinental Exchange, Inc.	A2	Securities Firms and Market Infrastructure Providers	Americas	High	$ 4,340
J.P. Morgan Securities, LLC	Aa3	Securities Firms and Market Infrastructure Providers	Americas	High	$ 309,678
Jefferies Group LLC	Baa3	Securities Firms and Market Infrastructure Providers	Americas	High	$ 20,186
Lazard Group LLC	Baa3	Securities Firms and Market Infrastructure Providers	Americas	High	$ 2,092
London Stock Exchange Group plc	A3	Securities Firms and Market Infrastructure Providers	Europe	High	$ 3,075
LPL Holdings, Inc.	Ba2	Securities Firms and Market Infrastructure Providers	Americas	High	$ 2,666
Mizuho Securities Co., Ltd.	A1	Securities Firms and Market Infrastructure Providers	Asia	High	$ 69,458
Morgan Stanley & Co. International plc	A1	Securities Firms and Market Infrastructure Providers	Europe	High	$ 112,108
Nasdaq, Inc.	Baa2	Securities Firms and Market Infrastructure Providers	Americas	High	$ 4,340
Nomura Holdings, Inc.	Baa1	Securities Firms and Market Infrastructure Providers	Asia	High	$ 230,637
Raymond James Financial, Inc.	Baa1	Securities Firms and Market Infrastructure Providers	Americas	High	$ 2,788
TD Ameritrade Holding Corporation	A2	Securities Firms and Market Infrastructure Providers	Americas	High	$ 2,950
Berkshire Hathaway Energy Company	A3	Electric Utilities	Americas	Med-High	$ 41,363
Duke Energy Corporation	Baa1	Electric Utilities	Americas	Med-High	$ 57,787
Electricite de France	A3	Electric Utilities	Europe	Med-High	$ 97,272
ENEL S.p.A.	Baa2	Electric Utilities	Europe	Med-High	$ 69,654

Company	Rating	Sector	Region	Cyber Risk Level	Total Debt ($MM)
ENGIE SA	A3	Electric Utilities	Europe	Med-High	$ 58,920
Iberdrola S.A.	Baa1	Electric Utilities	Europe	Med-High	$ 47,256
NextEra Energy, Inc.	Baa1	Electric Utilities	Americas	Med-High	$ 37,302
Saudi Electricity Company	A2	Electric Utilities	EMEA	Med-High	$ 49,873
Southern Company (The)	Baa2	Electric Utilities	Americas	Med-High	$ 47,808
Tokyo Electric Power Company Holdings, Inc.	Ba2	Electric Utilities	Asia	Med-High	$ 58,948
Aetna Inc.	Baa2	Health Insurance	Americas	Med-High	$ 8,800
Anthem, Inc.	Baa2	Health Insurance	Americas	Med-High	$ 20,156
Centene Corporation	Ba1	Health Insurance	Americas	Med-High	$ 7,514
Cigna Corporation	Baa2	Health Insurance	Americas	Med-High	$ 43,831
Humana Inc.	Baa3	Health Insurance	Americas	Med-High	$ 6,609
UnitedHealth Group Incorporated	A3	Health Insurance	Americas	Med-High	$ 39,871
WellCare Health Plans, Inc.	Ba2	Health Insurance	Americas	Med-High	$ 2,425
Boyd Gaming Corporation	B2	Lodging, Gaming and Cruise	Americas	Med-High	$ 4,775
Carnival Corporation	A3	Lodging, Gaming and Cruise	Americas	Med-High	$ 10,732
Genting Berhad	Baa1	Lodging, Gaming and Cruise	Asia	Med-High	$ 7,170
Las Vegas Sands Corp.	Baa3	Lodging, Gaming and Cruise	Americas	Med-High	$ 12,461
Marriott International, Inc.	Baa2	Lodging, Gaming and Cruise	Americas	Med-High	$ 11,438
MGM Resorts International	Ba3	Lodging, Gaming and Cruise	Americas	Med-High	$ 16,225
NCL Corporation Ltd.	Ba1	Lodging, Gaming and Cruise	Asia	Med-High	$ 6,613
Penn National Gaming, Inc.	Ba3	Lodging, Gaming and Cruise	Americas	Med-High	$ 9,894
Royal Caribbean Cruises Ltd.	Baa2	Lodging, Gaming and Cruise	Americas	Med-High	$ 11,306
Wyndham Destinations	Ba2	Lodging, Gaming and Cruise	Americas	Med-High	$ 5,581
3M Company	A1	Manufacturing & Auto	Americas	Med-High	$ 18,598
Beijing Automotive Group Co., Ltd.	Baa2	Manufacturing & Auto	Asia	Med-High	$ 18,824
Fiat Chrysler Automobiles N.V.	Ba1	Manufacturing & Auto	Europe	Med-High	$ 22,126
General Electric Company	Baa1	Manufacturing & Auto	Americas	Med-High	$ 76,763
General Motors Company	Baa3	Manufacturing & Auto	Americas	Med-High	$ 28,418
Honeywell International Inc.	A2	Manufacturing & Auto	Americas	Med-High	$ 20,366
Hyundai Motor Company	Baa1	Manufacturing & Auto	Asia	Med-High	$ 67,216
LafargeHolcim Ltd	Baa2	Manufacturing & Auto	Europe	Med-High	$ 19,702
Siemens Aktiengesellschaft	A1	Manufacturing & Auto	Europe	Med-High	$ 24,478
Volkswagen Aktiengesellschaft	A3	Manufacturing & Auto	Europe	Med-High	$ 68,100
Abbott Laboratories	A3	Medical Devices	Americas	Med-High	$ 23,208
Becton, Dickinson and Company	Ba1	Medical Devices	Americas	Med-High	$ 23,561
Boston Scientific Corporation	Baa2	Medical Devices	Americas	Med-High	$ 7,819
Danaher Corporation	A2	Medical Devices	Americas	Med-High	$ 11,698
Grifols S.A.	Ba3	Medical Devices	Europe	Med-High	$ 8,105
Medtronic, Inc.	A3	Medical Devices	Americas	Med-High	$ 29,468
Royal Philips N.V.	Baa1	Medical Devices	Americas	Med-High	$ 7,147
Stryker Corporation	Baa1	Medical Devices	Americas	Med-High	$ 11,412
Thermo Fisher Scientific Inc.	Baa1	Medical Devices	Americas	Med-High	$ 21,546
Zimmer Biomet Holdings, Inc.	Baa3	Medical Devices	Americas	Med-High	$ 9,611

Company	Rating	Sector	Region	Cyber Risk Level	Total Debt ($MM)
Amazon.com, Inc.	A3	Retail	Americas	Med-High	$ 70,832
CVS Health	Baa2	Retail	Americas	Med-High	$ 95,922
Home Depot, Inc. (The)	A2	Retail	Americas	Med-High	$ 35,333
Kroger Co. (The)	Baa1	Retail	Americas	Med-High	$ 26,859
Liberty Interactive LLC	Ba3	Retail	Americas	Med-High	$ 8,536
Lowe's Companies, Inc.	Baa1	Retail	Americas	Med-High	$ 20,559
Target Corporation	A2	Retail	Americas	Med-High	$ 13,489
Tesco Plc	Baa3	Retail	Europe	Med-High	$ 24,264
Walgreens Boots Alliance, Inc.	Baa2	Retail	Americas	Med-High	$ 40,744
Walmart Inc.	Aa2	Retail	Americas	Med-High	$ 75,521
Alibaba Group Holding Limited	A1	Technology	Asia	Med-High	$ 23,854
Apple Inc.	Aa1	Technology	Americas	Med-High	$ 157,901
Broadcom Cayman Finance Ltd.	Baa3	Technology	Americas	Med-High	$ 18,309
Intel Corporation	A1	Technology	Americas	Med-High	$ 33,854
International Business Machines Corporation	A2	Technology	Americas	Med-High	$ 31,028
Microsoft Corporation	Aaa	Technology	Americas	Med-High	$ 103,461
Oracle Corporation	A1	Technology	Americas	Med-High	$ 65,832
QUALCOMM Incorporated	A2	Technology	Americas	Med-High	$ 19,435
Tencent Holdings Limited	A1	Technology	Asia	Med-High	$ 27,686
Visa Inc.	Aa3	Technology	Americas	Med-High	$ 18,549
Altice Luxembourg S.A.	B2	Telecommunications & Media	Americas	Med-High	$ 40,370
AT&T Inc.	Baa2	Telecommunications & Media	Americas	Med-High	$ 223,677
Charter Communications, Inc.	Ba2	Telecommunications & Media	Americas	Med-High	$ 73,336
Comcast Corporation	A3	Telecommunications & Media	Americas	Med-High	$ 119,018
Deutsche Telekom AG	Baa1	Telecommunications & Media	Europe	Med-High	$ 95,817
Orange	Baa1	Telecommunications & Media	Europe	Med-High	$ 47,776
Sprint Corporation	B2	Telecommunications & Media	Americas	Med-High	$ 51,006
Telefonica S.A.	Baa3	Telecommunications & Media	Europe	Med-High	$ 72,178
Verizon Communications Inc.	Baa1	Telecommunications & Media	Americas	Med-High	$ 143,522
Vodafone Group Plc	Baa2	Telecommunications & Media	Europe	Med-High	$ 70,807
American Airlines Group Inc.	Ba3	Transportation Services	Americas	Med-High	$ 40,576
Burlington Northern Santa Fe, LLC	A3	Transportation Services	Americas	Med-High	$ 25,300
Central Japan Railway Company	A1	Transportation Services	Asia	Med-High	$ 46,018
CSX Corporation	Baa1	Transportation Services	Americas	Med-High	$ 15,757
Deutsche Post AG	A3	Transportation Services	Europe	Med-High	$ 22,425
East Japan Railway Company	Aa3	Transportation Services	Asia	Med-High	$ 34,114
FedEx Corporation	Baa2	Transportation Services	Americas	Med-High	$ 36,698
SNCF Mobilites	Aa3	Transportation Services	Europe	Med-High	$ 21,519
Union Pacific Corporation	Baa1	Transportation Services	Americas	Med-High	$ 25,842
United Parcel Service, Inc.	A2	Transportation Services	Americas	Med-High	$ 53,845

This table lists senior unsecured ratings for investment-grade companies and corporate family ratings for speculative-grade companies.
Total debt amounts are based on Moody's adjusted total debt as of the most recent fiscal year-end, except for Aetna Inc., which is as of 30 September 2018.
Source: Moody's Investors Service

Moody's related publications

Sector Comments

- Financial Institutions – South Korea: Korean banks bolster investment in cybersecurity, a credit positive, September 2019
- Exchanges and Clearing Houses – US: Options Clearing Corporation's risk management failures are credit negative, September 2019
- Medical products and devices – US: Innovation improves patient outcomes, but brings cyber risk and tech interlopers, July 2019
- For-Profit and Not-For-Profit Hospitals – US: Hospitals invest in data collection, telemedicine to reduce cost, July 2019
- Healthcare - US: Data breach at Quest and LabCorp highlights cyber risk in vendor relationships, June 2019
- Defense – US: Greater cybersecurity accountability for defense contractors would be credit negative, May 2019
- Financial Institutions – Europe: European financial authorities recommend cybersecurity legislation, a credit positive for financial institutions, April 2019

Sector In-Depth - Cyber

- Local government - US - Ransomware attacks highlight importance of IT investment and response planning, October 2019
- Hospitals & health service providers - US: Cyberattacks pose growing operational and financial risks for hospitals, September 2019
- Corporates - Global: Deepfake disinformation campaigns pose reputational risks to businesses, August 2019
- P&C Insurance — Global: Battling hidden cyber exposures, insurers position for growing opportunity, July 2019
- Electric and gas – US: Pipeline cybersecurity standards help plug security loophole in utility supply chain, July 2019
- Cross-Sector - Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019

Sector In-Depth - ESG

- Governance Considerations are a key determinant of credit quality for all issuers, September 2019
- Corporate governance assessments for publicly traded non-financial companies, July 2019

Topic pages

- Cyber Risk
- Environmental, Social and Governance (ESG)

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.

REPORT NUMBER 1193578

CLIENT SERVICES

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

MOODY'S
INVESTORS SERVICE