

SECTOR IN-DEPTH

12 November 2024



Contacts

Steven Libretti +1.212.553.1826
AVP-Cyber Credit Risk
steven.libretti@moodys.com

Sanja Nedic +33.6.2991.8072
AVP-Data Scientist
sanja.nedic@moodys.com

Leroy Terrelonge +33.1.5330.5989
Vice President - Cyber Credit Risk
leroy.terrelonge@moodys.com

Lesley Ritter +1.212.553.1607
SVP-Cyber Credit Risk
lesley.ritter@moodys.com

Fabian Astic +1.212.553.6814
Managing Director, Global Head of Digital Economy
fabian.astic@moodys.com

CLIENT SERVICES

Americas 1-212-553-1653

Asia Pacific 852-3551-3077

Japan 81-3-5408-4100

EMEA 44-20-7772-5454

Cybersecurity - Global

Our heat map shows sectors with \$7.1 trillion in debt face heightened cyber risk

Summary

Cyber risk in the telecommunications, airlines, and power generation industries shifts to the highest level in our latest cyber heat map. Numerous other sectors, including manufacturing, education, medical products, mass transit, and ports, also show more acute risk than in our [2022 heat map](#), either due to rising exposure or weaker oversight than in other industries. Together, these sectors account for \$7.1 trillion of debt. Our heat map uses both data and analytical insights to assess cyber risk in 71 industries globally. It shows rising risk across 16 industries. We score sector-level cyber risk on a four-level scale: Low, Moderate, High, or Very High.

Telecommunications and airlines join other critical infrastructure industries facing

Very High risk. Major telecom companies have experienced damaging cyberattacks in recent years, while the dependence of airlines on digital technology has made it vulnerable to operational disruption. Electric, gas and water utilities, and not-for-profit hospitals are also at the highest risk level. All these industries are highly digitized and play a crucial role in the functioning of society and the economy.

Eleven new industries shift to High risk. High risk and Very High risk sectors now represent \$28 trillion in debt. New High risk sectors include automobile manufacturers and suppliers, education, manufacturing, energy and ports. Greater risk at ports is illustrated by a slew of recent multiday disruptions in Japan and Australia. Higher education institutions have become more vulnerable due to comparatively weak defenses, while manufacturing sectors face rising risk due to increasing digitization of their production processes.

Growing digitization is driving increasing exposure to cyber risk. We now score two thirds of industries globally as highly or very highly digitized, bringing total rated debt in those classifications to 87%, from 74% in 2022. Underscoring the critical dependence of the various sectors on digital infrastructure and the extensive ramifications of such disruptions, was the July 2024 CrowdStrike incident where a defective software update led to the malfunction of millions of Windows devices in numerous industries globally.

Our cyber heat map assesses both exposure to cyber risk and cyber defense. We assess organizations' exposure to cyber risk (60%) and their preparedness to mitigate the risk (40%). Two components, their systemic role and digitization, make up the exposure factor. The mitigation factor has three components: perimeter integrity (protecting the integrity of a network's perimeter against cyberattack), cyber diligence, and cyber governance. Our assessment is for sectors and not individual debt issuers, so some issuers may have higher or lower exposure than their peers.

Sixteen sectors show heightened cyber risk in our 2024 heat map

Our latest cyber heat map points to higher cyber risk in 16 of the 71 sectors we assessed (Exhibit 1). Sectors with heightened cyber risk span a wide variety of industries including airlines, manufacturing and ports. Together, these sectors account for \$7.1 trillion of debt, representing 9% of Moody's \$82 trillion portfolio.

Exhibit 1

Cyber risk has risen in sectors representing \$7.1 trillion of debt

Sectors where cyber risk has moved higher or lower

Risk: ● Very High ● High ● Moderate ● Low

	2022 cyber risk score	2024 cyber risk score	Total 2024 debt (billions)
Airlines	●	●	\$1,600 moved up to Very High
Power generation projects	●	●	
Telecommunications	●	●	
Automobile manufacturers	●	●	\$4,385 moved up to High
Automotive suppliers	●	●	
Education and not-for-profits	●	●	
Finance companies	●	●	
Manufacturing	●	●	
Mass transit	●	●	
Medical products and devices	●	●	
Oil and gas – integrated oil companies	●	●	
Oil and gas – refining and marketing	●	●	
Ports	●	●	
Protein and agriculture	●	●	
Packaging manufacturers: metal, glass, and plastics	●	●	\$1,065 moved up to Moderate
Pharmaceuticals	●	●	\$932 moved down in risk
Media and entertainment	●	●	
Publishing	●	●	
Beverage industry	●	●	
Building materials	●	●	
Privately financed public infrastructure projects (PPPs)	●	●	

Source: Moody's Ratings

Two main factors are driving these higher cyber risk scores. These are firstly increased sector digitization, which introduces a more extensive digital footprint potentially more vulnerable to cyberattack, and secondly below-average cyber risk mitigation practices.

This publication does not announce a credit rating action. For any credit ratings referenced in this publication, please see the issuer/deal page on <https://ratings.moody's.com> for the most updated credit rating action information and rating history.

Heightened overall risk is accompanied by increased digitization for airlines, power generation projects, automobile manufacturers and suppliers, oil & gas refining and marketing, and ports. For other sectors digitization risks have stayed the same but are coupled with weakened defenses. These include education and not-for-profits, finance companies, manufacturing, mass transit, medical products and devices, integrated oil companies, and protein and agriculture industries.

A fuller explanation of the drivers underpinning changes in sector scores is available by accessing the cyber heat map data [here](#).

Telecommunications and airlines are among sectors rising to Very High risk

Cyber risk facing telecom firms, airlines, and power generation projects has risen to Very High in our latest heat map from High in 2022. With their addition, \$4.7 trillion of debt, representing eight sectors, now falls in the highest risk category (Exhibit 2).

Exhibit 2

Eight sectors with \$4.7 trillion in rated debt face Very High cyber risk
 Very High risk sectors in our cyber risk heat map, by value of debt (\$ billions)

Very High risk: **\$4,678B**



A detailed view of very high risk debt (billions), by sector

Telecommunications \$1,423	Electric and gas transmission and distribution \$693	Water and wastewater utilities \$419
Regulated and self-regulated utilities with generation \$1,104	Unregulated utilities and power companies \$582	Not-for-profit hospitals \$280
		Airlines \$129

Power generation projects: **\$48**

Source: Moody's Ratings

Sectors designated as Very High risk typically play an important systemic role and are highly digitized. The main distinction between these sectors and those rated as High lies in their systemic importance.

Cyberattacks on major telecommunications firms highlight the sector's vulnerability

The **Telecommunications** sector rises to the highest cyber risk category due to its systemic importance and broad digitization, along with weaker defense practices compared with other lower risk vital sectors.

Costly cyberattacks on companies such as [T-Mobile USA](#) (Baa2 stable), [AT&T Inc.](#) (Baa2 stable) and Optus Australia, a subsidiary of [Singtel Optus Pty Limited](#) (A3 stable) underscore the industry's Very High risk designation. These firms have experienced numerous and severe attacks in recent years that have resulted in the theft of personal information from millions of current and former customers and led to substantial financial settlements with regulators¹. The breaches illustrate the critical challenges telecommunications companies face in safeguarding sensitive customer data against increasingly sophisticated cyberattacks.

Telecommunications firms have made substantial investments in digital transformation, particularly in migrating significant portions of their operations to the cloud. While cloud services can reduce some cyber risks tied to the business, they may also introduce new vulnerabilities. This was evident in a recent [AT&T breach](#) where malicious actors gained access to data stored on a third-party cloud platform.

Although telecommunications companies are [investing heavily](#) in cybersecurity, their efforts have yet to counteract their heightened risk exposure. This stands in contrast to the very highly exposed banking sector, for instance, which despite facing similar risks, has more effectively mitigated the threat through implementation of top-tier cybersecurity measures. An example of weaker mitigation practices would be the telecommunications sector's vulnerability management where data from Moody's affiliate, Bitsight Technologies, points to the sector being 2.5 times more likely to have unaddressed Known Exploited Vulnerabilities (KEVs) ² affecting their networks than banks. The sector's cyber diligence and cyber governance scores similarly show weaker results in our [2023 cyber survey](#).

Heightened digitization of the airlines industry raises its risk to Very High from High

Airlines operate within a highly digital and increasingly interconnected ecosystem, rendering them susceptible to a range of cyber threats targeting sensitive customer data. Cybersecurity concerns include the potential for unauthorized access to flight control systems—despite high levels of security—and disruption to operational systems, such as aircraft and crew assignments, flight tracking and/or ticketing. Such incidents could inflict significant financial damage and tarnish a company's reputation. The industry's reliance on third-party software for many services introduces further vulnerabilities.

An example of the risk stemming from increased digitization is the incident involving [CrowdStrike Holdings Inc.](#) (Baa3 stable) in July 2024 where a defective software update led to the malfunction of millions of Windows devices globally. Even though this was not a cyberattack, the airlines industry was severely impacted, with carriers forced to cancel thousands of flights over several days. [Delta Air Lines](#) (Baa3 positive) was particularly hard hit and took over a week to resume normal operations. The company is facing substantial financial losses due to operational disruption, customer compensation, and a pending class-action lawsuit.

The sector's cyber risk mitigation as evaluated in this heat map shows weak results for digital perimeter integrity. Data from Bitsight indicates that the sector is among those most likely to display signs of networks compromised by potentially malicious programs or applications, leaving them more vulnerable to exploitation. Airlines also rank in the bottom third of sectors based on our assessment of their exposure to KEVs.

Cyber risk for not-for-profit hospitals and various utilities remains at Very High

Not-for-profit hospitals remain exposed to Very High cyber risk due to their reliance on digital technologies for patient care and the high value of sensitive health information they handle. Their essential role in patient care, with human lives at risk, underscores their systemic importance. Hospitals are more likely to pay ransoms to ensure their systems stay operational. The combination of potential loss of life and valuable patient data makes them attractive targets for cybercriminals.

The increasing complexity of hospital networks, with a multitude of interconnected devices and systems, further compounds these vulnerabilities. The rapid digital transformation in healthcare, often outpacing the implementation of corresponding [cybersecurity measures](#), exacerbates the situation. Consequently, the combination of valuable data, expanding attack surfaces, and the critical nature of hospital services contributes to the Very High cyber risk in this sector.

Two recent cyber event-related credit rating actions, [Mount Sinai Hospital NY's](#) downgrade from Baa1 to Baa3 with a negative outlook, and [Ascension Health Alliance's](#) (Aa2) outlook revision from stable to negative, highlight the credit risks they face.

Utilities, including electric and gas transmission and distribution, regulated and unregulated utilities, water and wastewater utilities also remain at Very High cyber risk. This is due to their role in critical infrastructure, making them attractive targets for sophisticated cyberattacks aimed at causing widespread disruption. A recent [spate of cyberattacks](#) on water and wastewater utilities, including [American Water Works Company, Inc.](#) (Baa1 stable), Southern Water Services Limited (Southern Water, funded through [SW \(Finance\) I PLC](#), Baa3 under review for downgrade), and South Staffordshire Water plc ([South Staffs Water](#), Baa2 stable), point to their vulnerability.

The integration of digital technologies and the presence of legacy systems increase vulnerabilities, while interconnected utility networks amplify the potential impact of any attack. Most utilities are very highly digitized. They are increasingly leveraging advanced

technologies such as smart grids, Internet of Things (IoT) devices and automated control systems to enhance operational efficiency and reliability. This digitization facilitates real-time monitoring and management of utility assets, but also introduces new cyber vulnerabilities.

Utilities attempt to offset these risks by deploying robust cyber governance and management programs, but due to large differences in scale and regulatory support for cybersecurity cost recovery, there is wide variability in individual utilities' ability to maintain the same level of investment as other corporations and financial institutions.

With the addition of 11 new sectors, High risk industries now represent \$23 trillion in debt

Eleven sectors move to the High risk category from Moderate. They include automobile manufacturers and their suppliers, education, manufacturing and ports (Exhibit 3). This takes total debt scored as either Very High or High cyber risk to \$28 trillion.

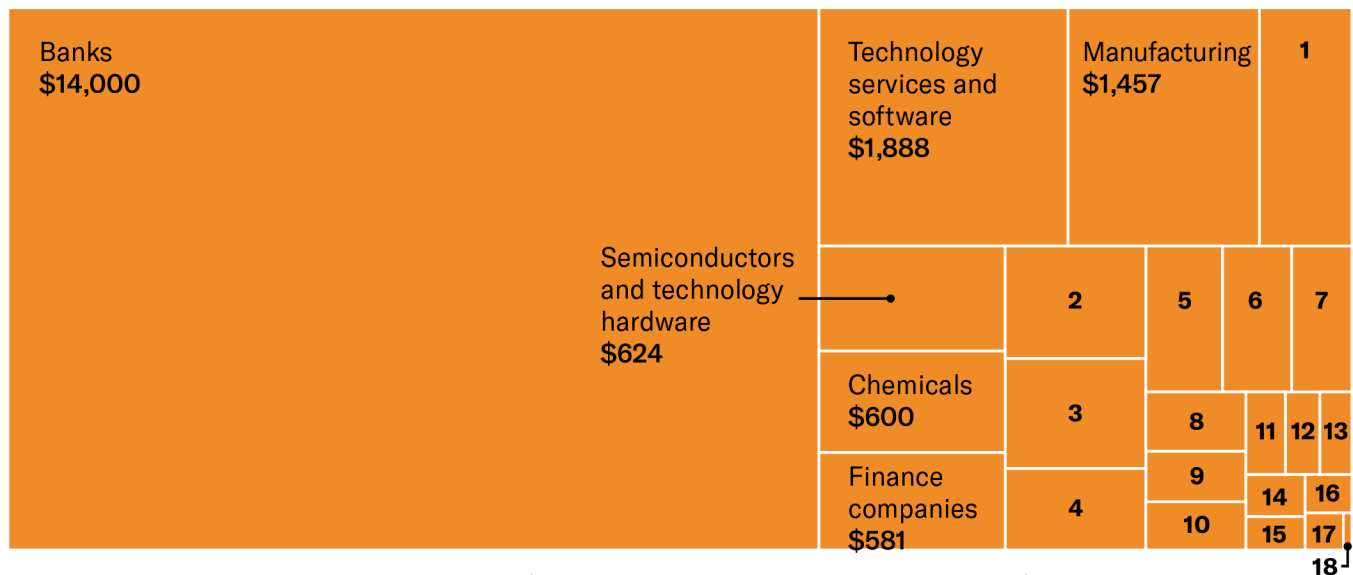
Exhibit 3

24 sectors with \$23.2 trillion in debt face High cyber risk
 High risk sectors in our cyber risk heat map, by value of debt (\$ billions)

Very High risk: \$4,678B



A detailed view of high risk debt (billions), by sector



- 1. Oil and gas – integrated oil companies: \$701
- 2. Automobile manufacturers: \$504
- 3. Oil and gas – midstream energy: \$489
- 4. Medical products and devices: \$365
- 5. Education and not-for-profits: \$356
- 6. Securities firms and market infrastructure providers \$321
- 7. Surface transportation and logistics: \$280
- 8. Distribution and supply chain services: \$187
- 9. Passenger railways: \$163
- 10. Automotive suppliers: \$154
- 11. Healthcare services – acute care and specialty services \$104
- 12. Trading companies: \$89
- 13. Mass transit: \$84
- 14. Oil and gas – refining and marketing: \$78
- 15. Equipment and transportation rentals: \$63
- 16. Protein and agriculture: \$58
- 17. Ports: \$46
- 18. Shipping: \$10

Source: Moody's Ratings

Sectors designated as High risk are typically highly reliant on digital technology to operate their business, but their systemic role is less critical than sectors in the Very High risk category.

Automakers face rising cyber risk due to greater digitization in vehicle production and operation. These firms rely heavily on fully automated manufacturing facilities whereby production lines are operated by computer systems, often with little human oversight. Automotive supply chains are highly complex and typically use electronic data interchange (EDI) systems (a method of exchanging

business documents electronically) to synchronize vehicle production with supplies of automotive parts. Auto manufacturers' exposure to cyber risk is further exacerbated by weak perimeter integrity and the systemically important role the sector sometimes plays as a significant contributor to the economic welfare of a certain region.

Education and not-for-profit institutions have become more vulnerable targets due to weak defenses. Universities, which are hubs of innovation and rich in valuable data, have become prime targets for cybercriminals. The education sector has reported one of the highest rates of ransomware attacks. Specifically, two thirds of education organizations [reported](#) a ransomware attack in 2023/2024. In addition, the costs of those incidents have more than tripled in the last year. Data from Bitsight and from our cyber survey show that they are not doing enough to mitigate the risks that come with high digitization. Entities in the education and not-for-profit sector are among the least prepared when it comes to protecting their network perimeters and executing basic cyber practices like multifactor authorization (MFA) and educating staff and students about cyber risk.

The **manufacturing** sector has increased its reliance on Industrial Control Systems and operational technology. These systems, which automate and operate industrial processes, were traditionally isolated but are now more connected. Many, however, were not designed with cybersecurity as a priority, rendering them susceptible to cyber threats. The sector's complex global supply chain introduces further vulnerabilities, as each vendor or partner can potentially bring new risks, allowing attackers to exploit weaker links to access more secure networks. Furthermore, the manufacturing sector is a repository of valuable intellectual property, making it an attractive target.

Our assessment shows that manufacturing organizations rank in the bottom 20% for perimeter integrity, leaving them exposed to known, exploitable software vulnerabilities. Additionally, our cyber survey responses indicate that, while large manufacturers have established strong cyber diligence practices, many small and mid-size organizations lack adequate cybersecurity measures due to budget constraints or a shortage of specialized personnel.

Ports are crucial to global trade and logistics, serving as key nodes in supply chains worldwide. Adoption of technologies like Internet of Things (IoT) devices for tracking containers, automation in loading and unloading processes, and digital platforms for managing shipping documentation have enhanced efficiency, but they also expand the attack surface for cybercriminals. Vulnerabilities in these systems can disrupt port activities, leading to significant financial losses and supply chain delays.

The complexity of port operations, involving multiple stakeholders, and their essential role in national economies further complicate cybersecurity efforts. A combination of increased digitization and weak cyber governance practices makes ports highly vulnerable, as highlighted by recent multiday disruptions in Japan and Australia. In July 2023, a ransomware attack hit Nagoya, Japan's largest port. Similarly, in November 2023, [DP World Australia](#) (Baa2 stable), which handles about 40% of the country's goods, had to halt operations at several ports due to a cyberattack.

Cyber risk declines in five sectors

Media & entertainment and **publishing** are now considered to be at Moderate risk (down from High in 2022), while **beverage industry**, **building materials**, and **privately financed public infrastructure projects** (PPPs) have moved from Moderate to Low risk. This change is driven by their lighter systemic roles and our increased emphasis on exposure, combined with above average mitigation scores.

Growing digitization is driving increasing exposure to cyber risk

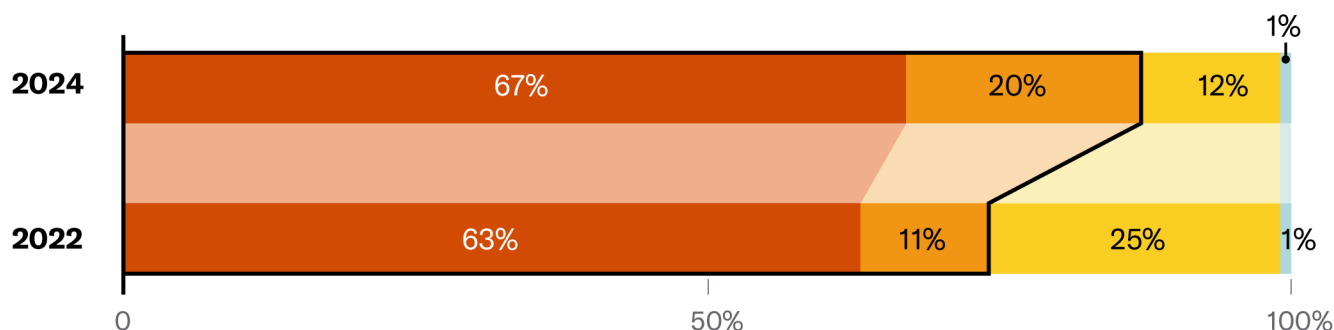
Our heat map shows increased digitization across 16 industries, making two thirds of industries now either highly or very highly digitized. Total debt classified under High or Very High digitization has risen to 87%, from 74% in 2022 (Exhibit 4).

Exhibit 4

The share of total debt with High or Very High digitization risk has increased to 87% from 74%



Digitization risk: ■ Very High ■ High ■ Moderate ■ Low



Source: Moody's Ratings

Digitization has also increased to High in six sectors without raising their overall cyber risk score. Those sectors include **Airports**, **Chemicals**, **Shipping**, **Surface Transportation and Logistics**, **Toll Roads**, and **Structured Finance**.

Airports have integrated advanced technologies to improve efficiency, security, and passenger experience. Digital systems now assist with check-in, security screening, and boarding, while RFID tags and barcodes have transformed baggage handling, enabling accurate tracking and automated sorting to minimize mishandling.

In the **chemicals** industry, increased digitization involves the use of IoT devices and sensors for real-time monitoring and control in production facilities. In the realm of chemical distribution, digitization extends to customer interactions through online platforms and mobile apps, offering customizable products and easier ordering. Digitization presents clear benefits for chemical companies, enhancing competitiveness, sustainability, and innovation in a complex global market.

The **shipping** industry has significantly ramped up its digitization efforts, integrating advanced technologies across various aspects of its operations to boost efficiency, enhance customer service, and streamline logistics. This digital transformation is evident through the adoption of automation and robotics for cargo handling, which not only minimizes human error but also ensures continuous operation, thereby increasing throughput.

In **surface transportation and logistics**, the embrace of digital technologies is multifaceted, incorporating advanced tracking and routing systems, cloud-based logistics platforms, and data analytics. GPS and IoT devices now enable real-time tracking of vehicles and cargo, providing up-to-the-minute updates on location, condition, and estimated arrival times, which significantly improves the precision of logistics operations.

Toll roads have seen increasing adoption of electronic toll collection (ETC) systems, such as RFID tags or transmission devices tied to accounts and license plate recognition technology, which eliminate the need for manual toll booths, reducing traffic congestion and lowering emissions from idling vehicles.

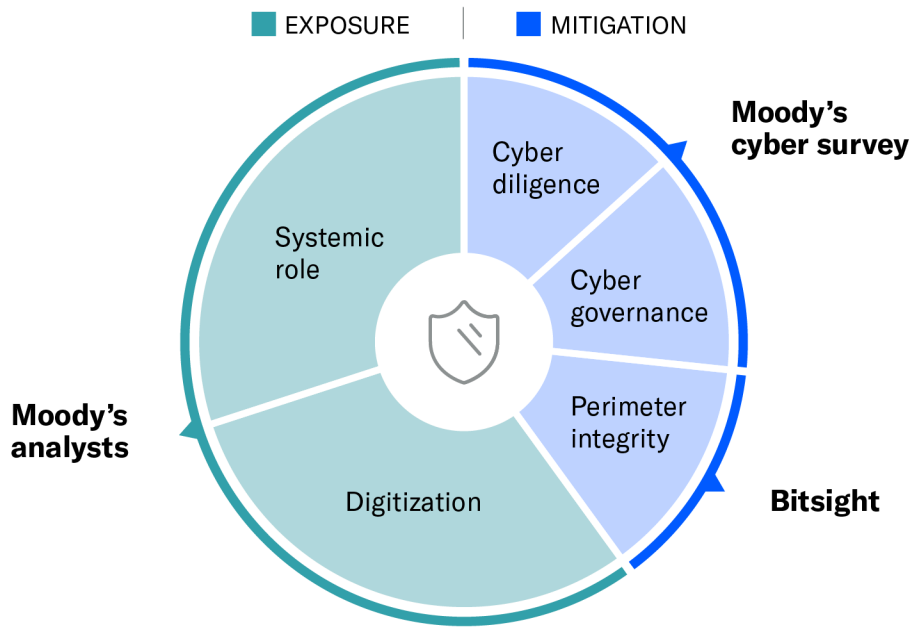
Digitization has become more apparent for **structured finance** transactions, particularly considering mortgage servicer cyberattacks in the last year that made it clear that the short-term inability to process payments is the primary way in which cyber risks could impact a structured finance deal.

Cyber risk is a function of exposure and mitigation

Our 2024 cyber heat map evaluates the cyber risk of 71 global industries using a four-level scale: Low, Moderate, High, or Very High (see Appendix B for definitions). This evaluation combines two components: exposure to cyber threats (60% of the overall score), balanced by cyber defense or mitigation (40%). This represents a shift from the equal weighting we assigned to exposure and mitigation in our 2022 cyber risk heat map. The shift underscores our evolving perspective that cyber risk is primarily determined by exposure due to a broadening threat landscape driven by rapid digitization. Meanwhile, mitigation efforts still play an important role in adjusting the overall risk profile by effectively reducing the impact of such exposures. The structure of our 2024 cyber heat map methodology is shown in Exhibit 5 below.

Exhibit 5

Cyber risk exposure, adjusted for risk mitigation data, drives our sector scores
 Two factors and five subcategories inform the scores



Sources: Moody's Ratings and Bitsight Technologies, Inc.

The **exposure** component assesses the attractiveness and vulnerability of organizations within an industry to cyberattacks. This assessment is qualitative, leveraging the expertise of analysts from Moody's Ratings. The **mitigation** component, on the other hand, evaluates the existence and effectiveness of cyber defense strategies in place. For this evaluation we rely on data from Bitsight, a cybersecurity ratings firm in which Moody's owns a minority stake, and the anonymized, aggregated findings from our [2023 issuer cyber survey](#).

Exhibit 6

Components of our cyber risk assessment

EXPOSURE: 60%

**Systemic role**

- The attractiveness of a sector as a cyber target for sophisticated attackers is in part informed by the ability to trigger knock-on effects for other sectors that could disrupt a whole region.
- A sector's systemic role depends on its level of interconnectivity with other sectors. The more other sectors rely upon it, the greater the systemic role is.
- A sector may also have a greater systemic role if there are only a handful of large issuers that dominate it.
- Utilities, telecommunications, not-for-profit hospitals, and banking sectors are scored as Very High on the systemic role risk scale.

**Digitization**

- A large digital footprint provides hackers with more "vectors" (or channels) to launch a cyberattack.
- Issuers that do business on the Internet are more susceptible to cyberattacks.

MITIGATION: 40%

**Perimeter integrity**

- Perimeter integrity measures the robustness of an organization's cybersecurity defenses at its network's outer edge, focusing on protection against unauthorized access, breaches, and cyber threats.
- Assessed using data provided by Bitsight through three key metrics: the presence of known exploited vulnerabilities (KEVs), botnet infections, and potentially malicious or unwanted software within the network.
- Banks and finance companies are among the best prepared. In contrast, sectors like education, mass transit, and manufacturing face the highest risk.

**Cyber diligence**

- Cyber diligence reflects how effectively an organization adopts and executes both fundamental and advanced cybersecurity practices, including employee training, vulnerability management, incidence response planning, and implementing multi-factor authentication (MFA), regular backups, tabletop exercises, and penetration testing.
- Evaluated using median responses from our 2023 issuer cyber survey.
- Banking, technology, and insurance sectors emerge as the best prepared, while consumer goods, education, and regional/local governments lag behind.

**Cyber governance**

- Cyber governance gauges an organization's commitment to cybersecurity, examining factors such as the employment of dedicated cyber personnel, cyber risk management reporting structures, board interaction frequency, long-term cyber risk strategies, and third-party cyber risk management.
- Evaluated using median responses from our 2023 cyber survey.
- Banking, insurance, and utilities sectors show high preparedness. Conversely, consumer goods, education, and mass transit are among the least prepared.











Sources: Moody's Ratings and Bitsight Technologies, Inc.

Appendix A

Scoring for sectors with Very High cyber risk - representing \$4.7 trillion of debt

Very High cyber risk sectors exhibit the highest level of cyber risk exposure, driven by their systemic importance and broad digitization, partially offset by moderate risk mitigation practices.

Risk: ● Very High ● High ● Moderate ● Low

	 Systemic role	 Digitization	 Perimeter integrity	 Cyber diligence	 Cyber governance	
Sector	2024 cyber risk score					
Airlines	●	●	●	●	●	●
Electric and gas transmission and distribution	●	●	●	●	●	●
Not-for-profit hospitals	●	●	●	●	●	●
Power generation projects	●	●	●	●	●	●
Regulated and self-regulated utilities with generation	●	●	●	●	●	●
Telecommunications	●	●	●	●	●	●
Unregulated utilities and power companies	●	●	●	●	●	●
Water and wastewater utilities	●	●	●	●	●	●

Scoring for sectors with High cyber risk - representing \$23.2 trillion of debt³

High cyber risk sectors exhibit high levels of exposure, typically driven by extensive digitization and a less important systemic role, partially offset by moderate cyber risk mitigation practices.

Risk: ● Very High ● High ● Moderate ● Low

Sector	2024 cyber risk score	Cyber risk factors				
		Systemic role	Digitization	Perimeter integrity	Cyber diligence	Cyber governance
Automobile manufacturers	●	●	●	●	●	●
Automotive suppliers	●	●	●	●	●	●
Banks	●	●	●	●	●	●
Chemicals	●	●	●	●	●	●
Distribution and supply chain services	●	●	●	●	●	●
Education and not-for-profits	●	●	●	●	●	●
Equipment and transportation rentals	●	●	●	●	●	●
Finance companies	●	●	●	●	●	●
Healthcare services – acute care and specialty services	●	●	●	●	●	●
Manufacturing	●	●	●	●	●	●
Mass transit	●	●	●	●	●	●
Medical products and devices	●	●	●	●	●	●
Oil and gas – integrated oil companies	●	●	●	●	●	●
Oil and gas – midstream energy	●	●	●	●	●	●
Oil and gas – refining and marketing	●	●	●	●	●	●
Passenger railways	●	●	●	●	●	●
Ports	●	●	●	●	●	●
Protein and agriculture	●	●	●	●	●	●
Securities firms and market infrastructure providers	●	●	●	●	●	●
Semiconductors and technology hardware	●	●	●	●	●	●
Shipping	●	●	●	●	●	●
Surface transportation and logistics	●	●	●	●	●	●
Technology services and software	●	●	●	●	●	●
Trading companies	●	●	●	●	●	●

Scoring for sectors with Moderate cyber risk - representing \$44.2 trillion of debt^{4,5}

Moderate cyber risk sectors exhibit average exposure, and comparatively stronger cyber risk mitigation practices.

Risk: ● Very High ● High ● Moderate ● Low

Sector	2024 cyber risk score	Systemic role	Digitization	Perimeter integrity	Cyber diligence	Cyber governance
Airports	●	●	●	●	●	●
Asset managers	●	●	●	●	●	●
Business and consumer services	●	●	●	●	●	●
Coal mining and coal terminals	●	●	●	●	●	●
Consumer goods	●	●	●	●	●	●
Environmental services and waste management	●	●	●	●	●	●
Gaming and gambling industry	●	●	●	●	●	●
Health insurance companies	●	●	●	●	●	●
Insurance brokers and service companies	●	●	●	●	●	●
Life insurance	●	●	●	●	●	●
Media and entertainment	●	●	●	●	●	●
Mortgage insurance	●	●	●	●	●	●
Packaging manufacturers: metal, glass, and plastics	●	●	●	●	●	●
Pension funds	●	●	●	●	●	●
Pharmaceuticals	●	●	●	●	●	●
Property, casualty and reinsurance	●	●	●	●	●	●
Publishing	●	●	●	●	●	●
Regional and local governments – advanced economies	●	●	●	●	●	●
Regional and local governments – emerging markets	●	●	●	●	●	●
Restaurants	●	●	●	●	●	●
Retail and apparel	●	●	●	●	●	●
Sovereigns – advanced economies	●	●	●	●	●	●
Sovereigns – emerging markets	●	●	●	●	●	●
Steel	●	●	●	●	●	●
Title and trade credit insurance	●	●	●	●	●	●
Tobacco	●	●	●	●	●	●
Toll roads	●	●	●	●	●	●

Scoring for sectors with Low cyber risk - representing \$9.8 trillion of debt

Low cyber risk sectors typically exhibit low exposure and comparatively stronger risk mitigation practices.

Risk: ● Very High ● High ● Moderate ● Low

Sector	2024 cyber risk score	Risk Factors				
		Systemic role	Digitization	Perimeter integrity	Cyber diligence	Cyber governance
Beverage industry	●	●	●	●	●	●
Building materials	●	●	●	●	●	●
Construction	●	●	●	●	●	●
Homebuilding and property development	●	●	●	●	●	●
Mining – metals and other materials, excluding coal	●	●	●	●	●	●
Oil and gas – independent exploration and production	●	●	●	●	●	●
Oil and gas – oilfield services	●	●	●	●	●	●
Paper and forest products	●	●	●	●	●	●
Privately financed public infrastructure projects (PPPs)	●	●	●	●	●	●
Public sector housing	●	●	●	●	●	●
Real estate trusts and other commercial property firms	●	●	●	●	●	●
Structured finance	●	●	●	●	●	●

Appendix B

Cyber risk scoring definitions and guidance

We score cyber risk on a four-point scale.

Very High risk	For sectors scoring Very High overall, the primary drivers are their high level of exposure to cyber risk and moderate risk mitigation practices. Elevated cyber risk exposure reflects these sectors' role as providers of critical services to the functioning of the broader economy, their high level of interconnectivity with other industries and their material reliance on digitization to operate their businesses. Sectors that score Very High on average tend to rely on moderate cyber risk mitigation practices, including comparatively strong cyber diligence and governance practices but somewhat weaker perimeter defenses.
High risk	For sectors scoring High overall, the primary drivers are their high level of exposure to cyber and moderate risk mitigation practices. Elevated cyber risk exposure reflects these sectors' role as providers of important services to the functioning of the broader economy or as suppliers to these critical providers, as well as their extensive reliance on digitization to operate their businesses. Sectors that score High on average tend to rely on moderate cyber mitigation practices, including comparatively strong cyber diligence but somewhat weaker cyber governance and perimeter defense practices.
Moderate risk	For sectors scoring Moderate overall, the primary drivers are their average exposure to cyber risk and comparatively strong risk mitigation practices. A moderate cyber risk exposure reflects the more localized, less interconnected nature of these sectors whereby a successful attack would not have wide ranging knock-on effects for the rest of the economy, but where there would still be material reliance on digitization to operate their businesses. Sectors that score Moderate on average tend to rely on comparatively strong cyber mitigation practices, including strong cyber diligence, governance and perimeter defense practices.
Low risk	For sectors scoring Low overall, the primary drivers are their low exposure to cyber risk and average cyber mitigation. A low cyber risk exposure reflects the localized nature of these sectors, whereby a successful attack would be unlikely to impact the rest of the economy. They also have a low reliance on technology and data to maintain business operations or an ability to easily revert to manual operations. Sectors that score Low on average tend to rely on relatively strong cyber mitigation practices, including strong perimeter defense practices and average cyber diligence and governance practices.

Endnotes

- 1 The frequency of cyber incidents at T-Mobile, in particular, led us to [lower their ESG Social Score](#) to S-4 (highly negative) from the S-3 (moderately negative) to reflect their increased customer relations risk.
- 2 Known Exploited Vulnerabilities (KEV) catalog is a [CISA maintained compilation](#) of known security vulnerabilities in software that have been exploited by bad actors in real-world scenarios.
- 3 For Education and not-for-profits, the perimeter integrity score is only based on KEV findings. We exclude Botnet Infections and Potentially Exploited data to avoid capturing erroneous data associated with guest networks.
- 4 Due to insufficient or unavailable data, Sovereigns and Regional and local governments - emerging markets risk mitigation scores are derived qualitatively.
- 5 For Airports, the perimeter integrity score is only based on KEV findings. We exclude Botnet Infections and Potentially Exploited data to avoid capturing erroneous data associated with guest networks.

© 2024 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 CREDIT RATINGS AFFILIATES ARE THEIR CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MATERIALS, PRODUCTS, SERVICES AND INFORMATION PUBLISHED OR OTHERWISE MADE AVAILABLE BY MOODY'S (COLLECTIVELY, "MATERIALS") MAY INCLUDE SUCH CURRENT OPINIONS. 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 APPLICABLE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S CREDIT RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS, NON-CREDIT ASSESSMENTS ("ASSESSMENTS"), AND OTHER OPINIONS INCLUDED IN MOODY'S MATERIALS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S MATERIALS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. AND/OR ITS AFFILIATES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS DO NOT COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS, ASSESSMENTS AND OTHER OPINIONS AND PUBLISHES OR OTHERWISE MAKES AVAILABLE ITS MATERIALS 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, ASSESSMENTS, OTHER OPINIONS, AND MATERIALS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS OR MATERIALS 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. FOR CLARITY, NO INFORMATION CONTAINED HEREIN MAY BE USED TO DEVELOP, IMPROVE, TRAIN OR RETRAIN ANY SOFTWARE PROGRAM OR DATABASE, INCLUDING, BUT NOT LIMITED TO, FOR ANY ARTIFICIAL INTELLIGENCE, MACHINE LEARNING OR NATURAL LANGUAGE PROCESSING SOFTWARE, ALGORITHM, METHODOLOGY AND/OR MODEL.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS 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 credit rating process or in preparing its Materials.

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, ASSESSMENT, 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 credit rating, agreed to pay to Moody's Investors Service, Inc. for credit ratings opinions and services rendered by it. MCO and Moody's Investors Service also maintain policies and procedures to address the independence of Moody's Investors Service credit ratings and credit rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold credit ratings from Moody's Investors Service, Inc. 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 under the heading "Investor Relations — Corporate Governance — Charter Documents - Director and Shareholder Affiliation Policy."

Moody's SF Japan K.K., Moody's Local AR Agente de Calificación de Riesgo S.A., Moody's Local BR Agência de Classificação de Risco LTDA, Moody's Local MX S.A. de C.V., I.C.V., Moody's Local PE Clasificadora de Riesgo S.A., and Moody's Local PA Clasificadora de Riesgo S.A. (collectively, the "Moody's Non-NRSRO CRAs") are all indirectly wholly-owned credit rating agency subsidiaries of MCO. None of the Moody's Non-NRSRO CRAs is a Nationally Recognized Statistical Rating Organization.

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 657AFSL 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 India only: Moody's credit ratings, Assessments, other opinions and Materials are not intended to be and shall not be relied upon or used by any users located in India in relation to securities listed or proposed to be listed on Indian stock exchanges.

Additional terms with respect to Second Party Opinions (as defined in Moody's Investors Service Rating Symbols and Definitions): Please note that a Second Party Opinion ("SPO") is not a "credit rating". The issuance of SPOs is not a regulated activity in many jurisdictions, including Singapore. JAPAN: In Japan, development and provision of SPOs fall under the category of "Ancillary Businesses", not "Credit Rating Business", and are not subject to the regulations applicable to "Credit Rating Business" under the Financial Instruments and Exchange Act of Japan and its relevant regulation. PRC: Any SPO: (1) does not constitute a PRC Green Bond Assessment as defined under any relevant PRC laws or regulations; (2) cannot be included in any registration statement, offering circular, prospectus or any other documents submitted to the PRC regulatory authorities or otherwise used to satisfy any PRC regulatory disclosure requirement; and (3) cannot be used within the PRC for any regulatory purpose or for any other purpose which is not permitted under relevant PRC laws or regulations. For the purposes of this disclaimer, "PRC" refers to the mainland of the People's Republic of China, excluding Hong Kong, Macau and Taiwan.

CLIENT SERVICES

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