MOODY'S INVESTORS SERVICE

Global Cyber Risk Issuer Surveys

SECTOR IN-DEPTH
24 April 2024

Send Your Feedback

TABLE OF CONTENTS

Contacts

Matthew Cahill, CFA +1.212.553.0299
AVP-Analyst
matt.cahill@moodys.com

Adam Hardi, CFA +1.416.214.3636
Vice President-Senior Analyst
adam.hardi@moodys.com

Adam Chaim, CFA +1.212.553.0086
VP-Senior Analyst
adam.chaim@moodys.com

Enoch Chu, CFA +1.212.553.4989
VP-Senior Analyst
enoch.chu@moodys.com

CLIENT SERVICES

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

Healthcare Providers – Global

2023 Cyber Survey shows strong healthcare defenses but ongoing investment needed

The healthcare sector maintains strong cyber defense practices, according to our latest cyber survey, with above-average implementation of advanced security measures such as vulnerability scans and penetration testing. The use of cyber insurance and third-party vendor management is strong for the industry, but the increasing complexity and digitization of the sector means that these risk mitigation strategies will remain a priority. Healthcare remains one of the top 10 sectors in terms of cyberattacks, which will require the industry to keep investing in cybersecurity at a time when it is under strain from rising expenses.

The observations in this report reflect survey responses and do not represent a definitive assessment of cybersecurity readiness.

» **Adoption of basic and advanced cyber practices in the industry is widespread.** Given its high cyber risk profile, the sector has largely adopted both basic and best cyber defense measures, such as multi-factor identification, penetration testing and vulnerability scans.

» **Cyber budgets and headcount continue to grow, reflecting sector exposure to attacks.** As cyberattacks become more sophisticated, continued investments will be needed to thwart hackers and mitigate the impact of successful attacks. Cyber spending as a share of IT reached 7% in 2023 up from 5% in 2019, while cyber headcount is up by 30%.

» **Providers continue to lean on cyber insurance to transfer risk, despite hefty premium increases.** Nearly all respondents carry cyber insurance, even though premiums for the sector have risen by 73% from 2021 to 2023, above the 49% global average increase for the period.

» **Management of risk from third-party vendors will require continued focus.** The extensive interconnection of the sector with third-party vendors requires strong oversight of these providers and their cyber practices. Favorably, 90% of healthcare issuers require a cybersecurity assessment of new vendors and 72% of vendors must undergo ongoing assessments.

» **Cyber governance is generally strong, but disclosure practices vary.** Healthcare issuers have a high proportion (94%) of dedicated cyber staff which reports to the C-suite. However, the level of cyber incident disclosure varies among healthcare subsectors.

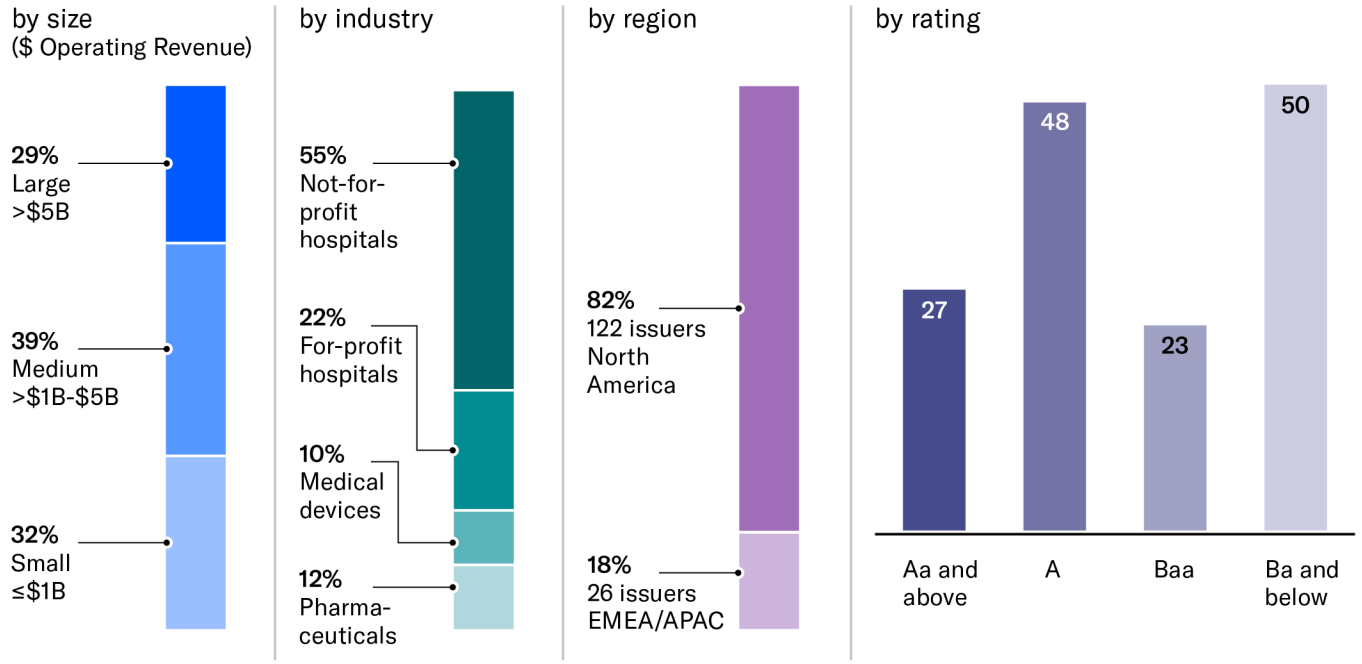
Based on our cyber heat map, we categorize not-for-profit healthcare as Very High Risk and for-profit healthcare as High Risk, reflecting their key systemic roles, high levels of digitization and information-rich databases. Cyber risk will remain elevated for the sector as the adoption of technology-driven patient care delivery, along with the industry's extensive use of third-party software, continues to grow. Increased digitization introduces new vulnerabilities for hackers to exploit through ransomware, data breaches and distributed denial-of-service (DDoS) attacks with the aim of interrupting medical operations or stealing sensitive patient data.

About our survey

Unlike most risks affecting healthcare organizations, cyber risk is indiscriminate and impacts all asset classes across all geographies. To better understand how cyber risk is evolving, and what private enterprises and government-related entities are doing to manage it, we conducted our second cybersecurity survey of organizations we rate. We collected nearly 2,000 responses globally, including 148 healthcare organizations. This report drills down into the responses we received, comparing them across four broadly defined sectors – Not-for-profit hospitals (55% of respondents), For-profit hospitals (22%), Medical devices (10%) and Pharmaceuticals (12%). In terms of the geographical distribution of the respondents, 122 were from North America (US and Canada), 25 from Europe, the Middle East and Africa (EMEA) and 1 from the Asia-Pacific region (APAC) (see Exhibit 1). We provide comparisons with all sector data (Global) as well as the Banking sector which is typically a frequent target of cyberattacks and has developed robust cyber defense practices.

Exhibit 1

Characteristics of healthcare sector respondents by size, sector, region and rating level



EMEA/APAC issuers include 25 issuers from EMEA and 1 issuer from APAC
Source: Moody's Ratings

Adoption of basic and advanced cyber practices in the industry is widespread

The industry has adopted many best practices in cyber defense. Examples include the use in most or all cases of multifactor authentication (98% adoption, up by about 4 percentage points on the 2021 survey), tabletop simulations (87%, up 17% points) and penetration tests (92%, up 18% points). All compare favorably with respondents globally. Nonetheless, hospitals and healthcare providers still plan to increase their investment in cyber defenses to protect patient data and ensure continuity of critical operations.

Our survey highlighted healthcare companies' use of several key cyber defense practices:

Basic defenses:

» **Incident response plans (IRPs).** These plans typically outline procedures to follow in the event of a security breach, the specific individuals required in the response, and their roles. IRPs are the foundation of cyber risk management, and 97% of healthcare survey respondents have such plans in place. An IRP is most effective when it is regularly tested, reviewed and updated. Most healthcare respondents (90% overall) indicated that they update and test their IRPs once a year. However, 8% of for-profit hospitals, 7% of pharmaceutical companies and 3% of not-for-profit hospitals report never testing their plans. Medical device companies all reported at least yearly testing. Further, 11% of small companies do not test or update their IRPs.

» **Tabletop exercises.** These exercises are used to test an organization's incident response plans, including its tools, procedures and proficiency in responding to different cyberattack scenarios. Survey respondents said they have broadly adopted tabletop exercises. Most healthcare companies (87%) said they conduct the exercises at least once a year, with for-profit hospitals reporting the lowest adoption (80%) compared with not-for-profit hospitals (87%), pharmaceutical companies (93%) and medical device companies (90%). Size was also a factor, as approximately 19% of small companies do not conduct tabletop simulations.

» **Cyber education for employees.** Education helps protect network entry points for cyberattacks, including external emails received by employees. All respondents reported engaging with and educating personnel at least yearly, and about half engage with employees monthly.

» **Regular backups of an organization's network.** Backups are an effective way to rapidly restore operations after a ransomware attack. Ransomware typically encrypts a target's files, hampering their operations until a ransom key is provided by the attacker or the target restores its systems using existing backups. Most healthcare companies perform these backups at least weekly, although 9% of medical device companies report only doing backups monthly and 4% of not-for-profit hospitals report doing so only yearly.

Intermediate/advanced defenses:

» **Vulnerability scans.** These scans detect known exploitable weaknesses across an organization's network, computers and applications. Automated vulnerability scanning tools are widely available from a number of security vendors and are often bundled with other security software. Survey respondents reported universal use of vulnerability scans.

» **Penetration testing (pen testing).** This testing simulates a cyberattack to assess an organization's designated applications and networks. Pen testing is another important program to evaluate cyber resilience. Penetration testing typically uses a combination of automated and manual testing. While the industry as a whole conducts annual pen tests more often than average (healthcare 92% at least annually as opposed to 88% globally), within the healthcare subsectors, for-profit hospitals and not-for-profit hospitals lag with 12% and 9%, respectively, reporting either infrequent testing (every few years) or never conducting these tests at all. Further, medium and small companies also did not consistently perform pen testing at least annually.

» **Red team/purple team testing.** These tests are a broader form of penetration testing that typically involve an internal or external team that uses targeted real-life attacks to test an organization's physical and cybersecurity defenses and incident response plans. Red team/purple team testing tends to be used by organizations with more mature or advanced security postures. Adoption of red team/purple team (55% for healthcare) remains lower than banks, a similarly high cyber risk sector (68%), but above the global average (47%). There is a wide variation in the healthcare sector, with medical device companies reporting at least annual red/purple team tests 60% of the time and pharmaceutical company respondents reporting at least annual tests 83% of the time. Only 42% of the for-profit and 53% of not-for-profit hospital respondents said they had conducted a red team/purple team test in the previous 12 months.

Exhibit 2

Strong cyber defense practices have been widely implemented in the healthcare sector

	Sector Comparison			Healthcare Subsector Comparison			
Operations	Global	Banks	Healthcare	Not-for-Profit hospitals	For-profit hospitals	Medical products	Pharma-ceuticals
Issuer engages with or educates personnel on cybersecurity issues at least annually	98%	99%	100%	100%	100%	100%	100%
Merger and acquisition proposals require a risk assessment from the team responsible for the issuer's cybersecurity	78%	87%	78%	81%	86%	42%	83%
Issuer uses multi-factor authentication (MFA) to manage remote access to internal resources, such as email	90%	90%	98%	100%	96%	100%	93%
Issuer has a patch management policy	95%	95%	100%	100%	100%	100%	100%
Issuer backs up its data and/or systems to a resource that is disconnected from the issuer's network (at least monthly)	97%	96%	97%	96%	100%	100%	100%
Issuer conduct tabletop simulations (at least annually)	76%	91%	87%	87%	80%	90%	93%
Issuer conducts penetration tests (at least annually)	88%	96%	92%	91%	88%	100%	100%
Issuer conducts red team/purple team engagements (at least annually)	47%	68%	55%	53%	42%	60%	83%

Source: Moody's Ratings

Cyber budgets and headcount continue to grow, reflecting prevalence of attacks

Hospitals in particular face financial challenges that will make investment in cybersecurity more difficult. Labor shortages, exacerbated by the pandemic, have put upward pressure on wages and restrained growth in margins. Higher inflation and supply chain disruptions have also increased costs. Additionally, higher interest rates have raised the cost of debt and made financing equipment or investing in capital more expensive.

Nevertheless, spending by healthcare providers on cybersecurity management has risen since 2019, keeping pace with global trends. As a percentage of total technology budgets, cyber spending climbed to an estimated 7% in 2023 from 5% in 2019 (Exhibit 3). In their budgets, 81% of healthcare issuers have cybersecurity as a line item compared with 74% of issuers globally.

The growth in cyber budgets has, in turn, given most industries the means to grow their in-house cyber expertise. Over the three-year period from 2019 to 2022, there was a 30% increase in the number of full-time cybersecurity employees across healthcare, which is consistent with the global average (30%) and banks (29%). Among its many advantages, in-house cyber expertise is beneficial to an organization because it limits the number of third parties accessing the organization's corporate network, reducing the organization's digital footprint. However, survey results show hospitals are also outsourcing cybersecurity employees, with an increase of 50% in the number of outsourced employees from 2019 to 2022, markedly higher than the global average of 15% and above banks (41%).

Exhibit 3
Cyber budgets as a percentage of IT spending continue to grow

	Sector Comparison			Healthcare Subsector Comparison			
	Global	Banks	Healthcare	Not-for-profit hospitals	For-profit hospitals	Medical devices	Pharma-ceuticals
% of the issuer's total technology budget allocated to cybersecurity for 2019	5	5	5	5	9	5	5
% of the issuer's total technology budget allocated to cybersecurity for 2023	8	8	7	6	9	7	6
Total % change in number of non-outsourced cybersecurity employees 2019-2022	30	29	30	25	50	1	28
Total % change in number of contract or outsourced cybersecurity employees 2019-2022	15	41	50	11	67	0	151

Source: Moody's Ratings

Management of third-party vendors stands above other corporate and public sectors

The growing interconnectedness of healthcare delivery and the increasing reliance on technology will increase the need for strong cyber defenses. The extensive use of third-party software vendors for clinical operations and record keeping, billing and other functions will add to the sector's cyber risk, and the expanding adoption of remote care and work beyond physically controlled borders will yield additional vulnerabilities.

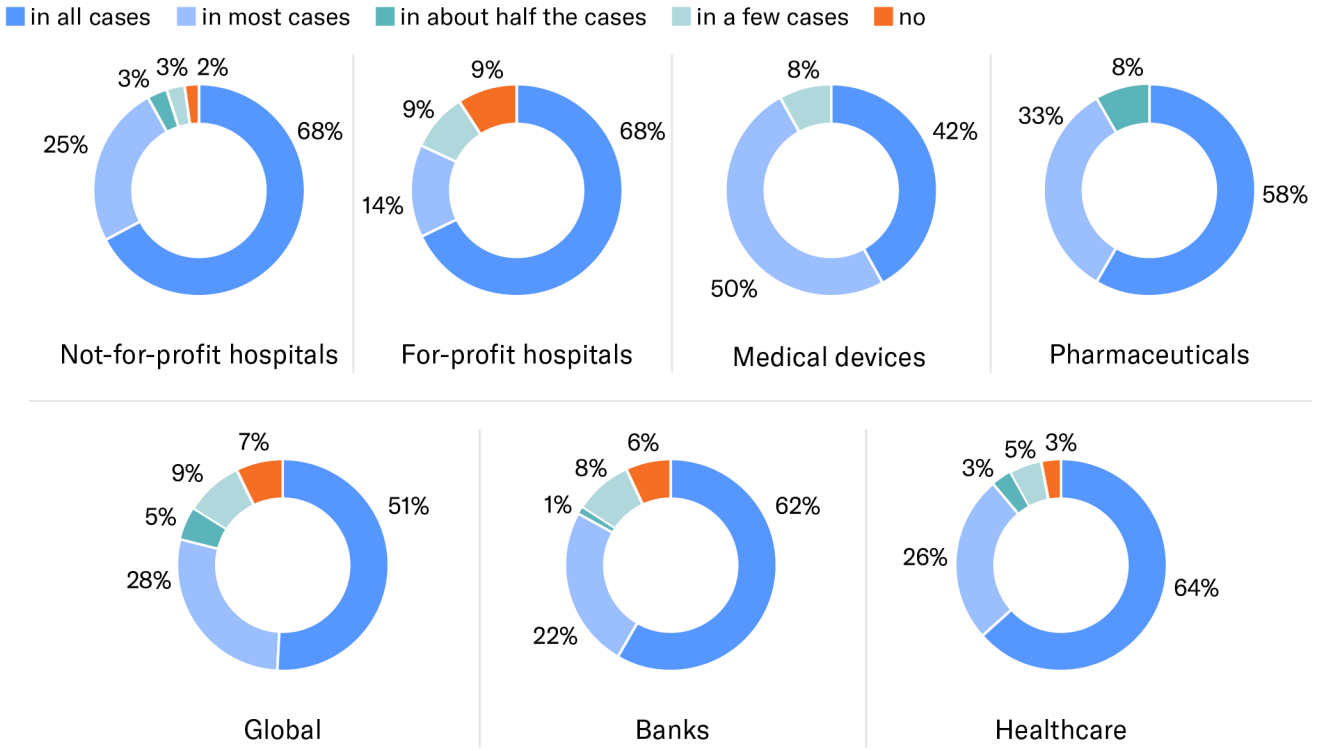
Security breaches among connected third-party providers are prompting customers to reevaluate their vendors. In February 2024, a cyberattack shut down Change Healthcare (Change), a part of UnitedHealth Group (A2 stable). Change provides clearinghouse services that allow healthcare providers to electronically submit insurance claims and receive payments. A large share of providers were affected by the attack, leading to delays in reimbursement, pharmacy services and pretreatment authorizations.

In our survey, about 90% of healthcare issuers said they required a cybersecurity assessment of new vendors, either most of the time (26%) or all the time (64%), as shown in Exhibit 4. These results are notably stronger than for their global peers and the banking industry, which report performing new vendor cyber assessments in most cases – 79% and 84% respectively.

Exhibit 4

Healthcare respondents conduct more frequent initial cyber assessments of third-party vendors than banking or global peers

Are new vendors subject to an initial cyber assessment?



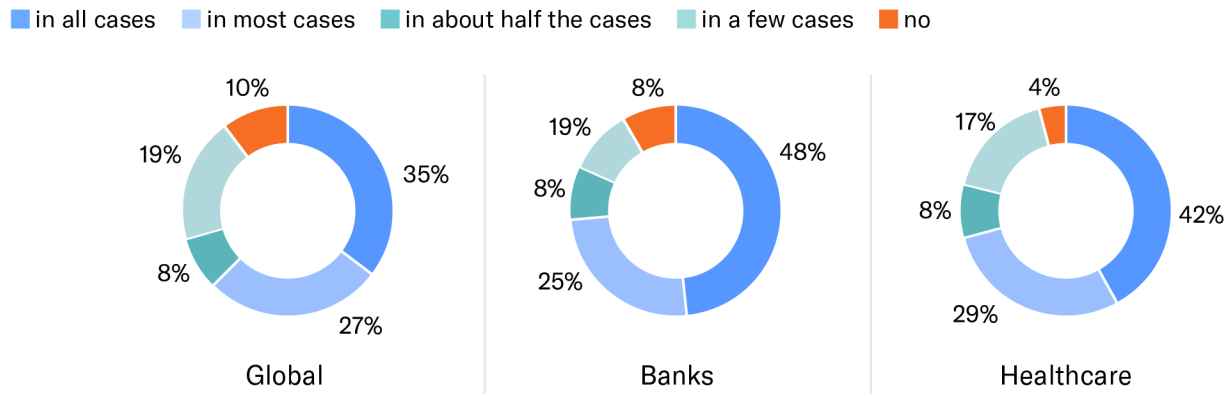
Source: Moody's Ratings

Current vendors are subject to periodic cybersecurity review more frequently in healthcare than in other sectors. Some 72% of healthcare respondents conduct ongoing reviews (42% always and 29% in most cases) compared with 63% (35% and 27%) of global peers and 74% of banks (48% and 25%). However, these reviews represent a marked drop-off from the initial screening process. Moreover, 5% of not-for-profit hospitals and for-profit hospitals reported never doing an ongoing review of third-party vendors – a weak performance given that not-for-profit issuers represent critical infrastructure and are one of the industries most targeted by hackers (see Exhibit 5).

Exhibit 5

Ongoing review of third-party vendors is less frequent than initial screening

Are vendors subject to periodic review of cybersecurity?



Source: Moody's Ratings

Cyber insurance, a key risk management tool for many organizations, is not universally required for healthcare third-party vendors, though 69% of providers require vendors whose personnel or products have access to the organization's computer systems to carry coverage. This is significantly higher than both global peers (37%) and the banking sector (25%). The higher coverage likely reflects the complexity of healthcare providers' digital networks and their extensive dependence on a patchwork of third-party vendors with access to their networks.

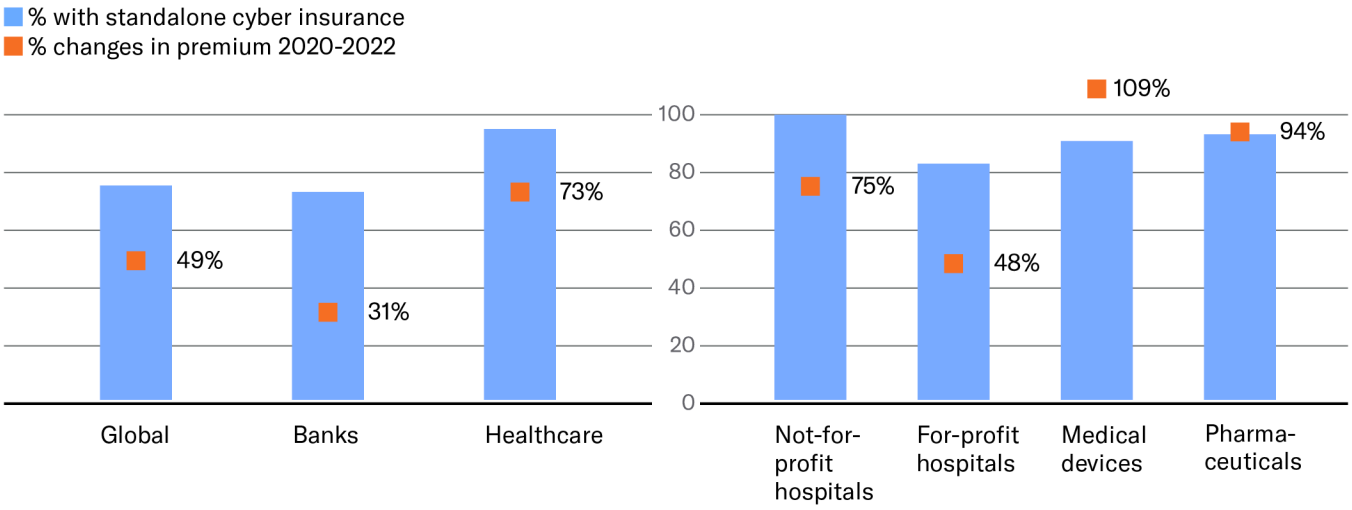
Healthcare relies heavily on standalone cyber insurance for risk mitigation

Healthcare primarily uses cyber insurance to mitigate risk, despite rising costs and often declining insurance limits and coverages. A very high 95% of respondents carry cyber insurance, exceeding the global average of 75% and in line with the 94% reported in the 2021 Cyber Survey (see Exhibit 6). Only for-profit hospitals and providers in EMEA had lower adoption rates at 83% and 80%, respectively.

Indeed, healthcare providers continue to opt for cyber insurance even as premiums have increased faster over the past two years than for other sectors: up 73% compared with the 49% average increase among all respondents. Further, demand for more insurance remains strong, particularly at medium and smaller healthcare companies, where 23% and 16% of respondents said they planned to increase their coverage in the coming year. Insurers have faced larger, more frequent claims due to ransomware attacks, significantly weakening their product's profitability. Tighter terms and conditions, as well as costlier premiums, have sent the cost of transferring risk higher.

Exhibit 6

Despite rapidly rising premiums, more healthcare companies carry standalone cyber insurance than banks and global peers



Percentage change in premium represents reported percentage change between 2020 and 2022.
Source: Moody's Ratings

It is not surprising that healthcare has widely adopted cyber insurance: the sector is likely to see an increase in class-action lawsuits as a result of data breaches. Healthcare has a higher amount of legal settlements covered by insurance policies (75%) than the global average (63%). However, despite the frequency of ransomware attacks, less than half of healthcare companies have ransom payments included in their traditional insurance policies, which likely explains the widespread use of standalone policies (see Exhibit 7).

Exhibit 7

Traditional coverage leaves vulnerabilities, driving adoption of standalone cyber insurance

Percentage of issuers whose traditional insurance policy explicitly includes a particular type of cyber coverage

	Sector Comparison			Healthcare Subsector Comparison			
	Global	Banks	Healthcare	Not-for-profit hospitals	For-profit hospitals	Medical devices	Pharma-ceuticals
Business interruption	77	70	76	80	71	75	67
Contingent business interruption	56	50	70	70	71	75	67
Regulatory fines	57	56	67	71	76	63	33
Reputational damage	58	50	74	73	88	75	58
Funds transfer fraud	43	35	53	59	59	38	25
Incident response	77	73	81	80	94	75	67
Legal settlements	63	57	75	80	76	63	58
New equipment	43	35	51	55	41	38	50
Property damage	39	47	42	46	29	25	50
Ransom payments	72	64	81	82	100	75	50

Source: Moody's Ratings

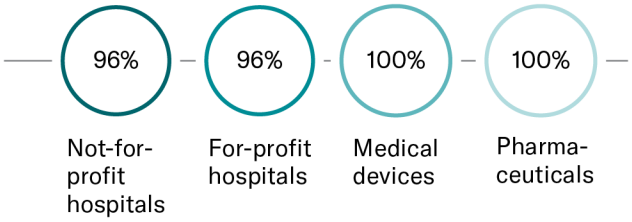
Cyber governance widely viewed as important at board level, yet disclosure practices vary

Strong cyber governance is instrumental in implementing an effective enterprise-wide approach to cybersecurity. Proximity in an organization's reporting structure of the person responsible for cybersecurity to the top executive team is one indicator of strong governance. Overall, the healthcare sector showed strong cyber alignment, with 94% of respondents having a dedicated cyber staff and 92% a cyber manager who reports directly to the C-suite (see Exhibit 10). However, 15% of smaller issuers, and 21% of issuers in EMEA, did not have a dedicated cyber employee.

In addition to reporting to the C-suite, most entities brief the board of directors, though there is room for improvement in this area, especially given the high risk of cyberattacks in the sector. Nearly a quarter of healthcare entities do not provide at least annual briefings to the board from a senior cyber manager (see Exhibit 9).

Exhibit 8

Among nearly all respondents, CEOs receive direct briefings from senior cyber managers at least annually...

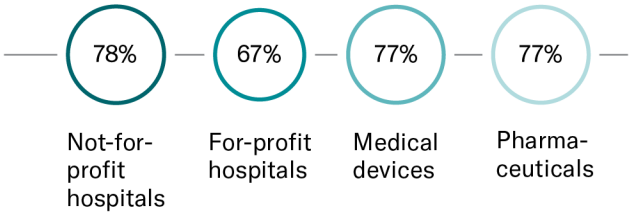


Source: Moody's Ratings

Exhibit 9

...but updates to boards of directors present an area of opportunity

Percentage of respondents whose entire board of directors receive at least an annual update from a senior cyber manager



Source: Moody's Ratings

Public disclosure of cyber incidents is strong among healthcare respondents, likely due to the fact that the US Department of Health and Human Services, requires that health organizations disclose cyber breaches that impact more than 500 people. Some 27% reported a cyber incident to their customers over the past two years, higher than the global survey average of 21%. Pharmaceuticals had the lowest disclosure rate of 14%. Not-for-profit healthcare providers issued nearly double the global average of public notices of cyber incidents – 42% compared with 22% (see Exhibit 10).

Exhibit 10

Disclosure practices vary among sectors, with incident reporting to customers and regulators lagging internal reporting practices

	Sector Comparison			Healthcare Subsector Comparison			
Governance	Global	Banks	Healthcare	Not-for-Profit hospitals	For-profit hospitals	Medical products	Pharma-ceuticals
Issuer has cyber incident reporting requirements for incidents that do not result in the disclosure of personally identifiable information (PII)	66%	92%	67%	63%	64%	80%	85%
Issuer has issued a public notice of a cyber incident	22%	24%	34%	42%	32%	18%	7%
Issuer has reported a cybersecurity incidents it has experienced to regulators over the past 2 years	27%	49%	28%	29%	24%	30%	31%
Issuer has reported any cybersecurity incidents to its customers over the past 2 years	21%	19%	27%	30%	26%	27%	14%
Issuer has reported a cybersecurity incidents to its board/council over the past 2 years	46%	58%	50%	44%	46%	64%	77%
Issuer has employees whose primary responsibility is cybersecurity	86%	97%	94%	99%	90%	87%	89%
Senior cyber manager reports to c-suite	90%	95%	92%	90%	89%	100%	100%

Source: Moody's Ratings

Appendix

Exhibit 11

	Global	Global Banks	Global Healthcare	Global Healthcare Sectors			
				Not-for-profit hospitals	For-profit hospitals	Medical devices	Pharmaceuticals
Number of responses	**1,992**	**224**	**148**	**82**	**33**	**15**	**18**
GOVERNANCE							
Does the issuer have employees whose primary responsibility is cybersecurity?	86%	97%	94%	99%	90%	87%	89%
To whom does the senior cyber manager report?							
c-suite employee	90%	95%	92%	90%	89%	100%	100%
an employee not in the c-suite	10%	5%	8%	10%	11%	0%	0%
Does compensation for the issuer's chief executive depend on meeting defined cybersecurity performance objectives?	18%	39%	16%	15%	21%	0%	23%
How often does the issuer's chief executive receive direct briefings from the senior cyber manager?							
monthly or more	45%	55%	41%	49%	42%	0%	31%
quarterly or more, but less frequently than monthly	35%	31%	36%	33%	35%	50%	46%
semiannually or more, but less frequently than quarterly	9%	9%	13%	8%	8%	42%	23%
yearly or more, but less frequently than semiannually	7%	3%	6%	5%	12%	8%	0%
less frequently than yearly	2%	1%	2%	3%	0%	0%	0%
never	3%	1%	2%	1%	4%	0%	0%
How many times per year does the senior cyber manager directly report on cybersecurity to the entire Board of Directors?							
monthly or more	6%	13%	1%	0%	4%	0%	0%
quarterly or more, but less frequently than monthly	27%	41%	17%	14%	26%	8%	31%
semiannually or more, but less frequently than quarterly	19%	15%	26%	29%	19%	31%	23%
yearly or more, but less frequently than semiannually	27%	23%	31%	36%	19%	38%	23%
less frequently than yearly	8%	2%	10%	10%	11%	8%	8%
never	14%	5%	15%	12%	22%	15%	15%
How often does the senior cyber manager directly report on cybersecurity to a committee of the Board of Directors?							
monthly or more	8%	17%	0%	0%	0%	0%	0%
quarterly or more, but less frequently than monthly	43%	56%	43%	50%	36%	33%	25%
semiannually or more, but less frequently than quarterly	18%	12%	30%	26%	16%	42%	67%
yearly or more, but less frequently than semiannually	15%	9%	16%	15%	24%	17%	0%
less frequently than yearly	5%	2%	2%	1%	8%	0%	0%
never	11%	4%	9%	7%	16%	8%	8%
What percentage of the issuer's board members have cybersecurity expertise?	10%	20%	10%	8%	18%	15%	10%
What percentage of the issuer's board members have experience helping a company respond to and/or recover from a cyber incident?	10%	19%	10%	6%	30%	50%	8%
Which committee of the Board of Directors (or equivalent governing body) is responsible for oversight of cybersecurity?							
audit	33%	4%	55%	58%	43%	62%	50%
risk	21%	53%	14%	14%	4%	15%	29%
cybersecurity/cyber risk	11%	16%	7%	3%	17%	8%	7%
technology	15%	11%	5%	3%	17%	0%	0%
other	21%	15%	20%	23%	17%	15%	14%
Does the issuer assess cyber risk in terms of financial impact (often called "cyber risk quantification")?	63%	80%	64%	71%	50%	46%	67%
How does the issuer assess cyber risk in terms of financial impact?							
we conduct this analysis internally	57%	76%	48%	37%	67%	88%	56%
we leverage our cyber insurance underwriting process	23%	6%	32%	42%	25%	0%	11%
we use an external vendor product	10%	6%	14%	15%	0%	13%	22%
other	10%	12%	6%	6%	8%	0%	11%
Does the issuer communicate cyber risk in terms of financial impact to its board/council?	78%	85%	72%	78%	40%	86%	60%
Has the issuer determined a maximum acceptable financial loss amount from a cyber incident (often called a "cyber risk appetite")?	41%	65%	42%	55%	17%	25%	43%
Is the issuer's cyber risk appetite reviewed by its board/council?	85%	97%	82%	84%	75%	100%	67%

	Global	Global Banks	Global Healthcare	Global Healthcare Sectors			
				Not-for-profit hospitals	For-profit hospitals	Medical devices	Pharmaceuticals
OPERATIONS							
Is cyber risk centrally managed across issuer's subsidiaries, or managed separately by each subsidiary?							
centrally managed	89%	84%	97%	100%	85%	100%	100%
managed separately	11%	16%	3%	0%	15%	0%	0%
Does the issuer characterize the cyber assets most critical to its operations as information technology or operational technology assets?							
primarily IT	41%	58%	34%	36%	48%	25%	7%
primarily OT	4%	2%	4%	1%	7%	8%	7%
both	55%	41%	62%	62%	44%	67%	87%
Does the issuer have a multi-year roadmap or strategy for managing cyber risk?	89%	94%	94%	94%	92%	100%	93%
Total % change in number of non-outsourced cybersecurity employees 2019-2022	30%	29%	30%	25%	50%	1%	28%
Total % change in number of contract or outsourced cybersecurity employees 2019-2022	15%	41%	50%	11%	67%	0%	151%
Does cybersecurity have its own line item in the issuer's budgeting process?	74%	80%	81%	81%	74%	92%	86%
What percentage of the issuer's total technology budget was or is projected to be allocated to cybersecurity for 2019?	5%	5%	5%	5%	9%	5%	5%
What percentage of the issuer's total technology budget was or is projected to be allocated to cybersecurity for 2020?	6%	6%	5%	5%	8%	5%	6%
What percentage of the issuer's total technology budget was or is projected to be allocated to cybersecurity for 2021?	6%	8%	6%	5%	8%	5%	5%
What percentage of the issuer's total technology budget was or is projected to be allocated to cybersecurity for 2022?	8%	7%	7%	6%	10%	7%	6%
What percentage of the issuer's total technology budget was or is projected to be allocated to cybersecurity for 2023?	8%	8%	7%	6%	9%	7%	6%
Total % change in amount was or is projected to be spent on cybersecurity 2019-2023	71%	50%	50%	41%	54%	141%	25%
How does the issuer monitor for and/or detect cyber incidents?							
internal security operations center (SOC)	28%	38%	20%	19%	20%	42%	7%
managed security service provider (MSSP)	18%	10%	14%	15%	16%	25%	0%
no monitoring/detection capability	2%	1%	1%	0%	4%	0%	0%
both mssp and soc	48%	46%	63%	65%	56%	33%	93%
other	5%	4%	2%	1%	4%	0%	0%
Does the issuer participate in industry threat information sharing groups?	85%	94%	92%	95%	93%	83%	86%
Does the issuer have a vulnerability management program?	95%	98%	97%	97%	96%	92%	100%
Has the issuer developed an incident response plan that includes cyber incidents?	95%	100%	97%	99%	96%	92%	93%
How often does the issuer test the incident response plan?							
more than 4 times a year	8%	9%	9%	12%	4%	0%	7%
four times a year	6%	7%	8%	10%	4%	0%	7%
three times a year	3%	6%	2%	1%	0%	0%	7%
twice a year	17%	18%	20%	24%	16%	10%	14%
once a year	53%	57%	52%	43%	60%	90%	57%
every few years	8%	2%	6%	7%	8%	0%	0%
never	6%	2%	4%	3%	8%	0%	7%
How often does the issuer review the incident response plan for potential updates?							
more than 4 times a year	9%	8%	8%	11%	4%	0%	7%
four times a year	7%	5%	13%	11%	13%	20%	20%
three times a year	2%	4%	3%	3%	0%	10%	0%
twice a year	14%	9%	15%	13%	25%	0%	20%
once a year	59%	75%	54%	54%	54%	70%	47%
every few years	6%	1%	4%	7%	0%	0%	0%
never	3%	0%	3%	1%	4%	0%	7%
Does the issuer have an insider threat program to detect and mitigate threats from employees and other individuals with access to the issuer's systems, data, or premises?	75%	87%	74%	77%	60%	58%	100%
How often does the issuer engage with or educate personnel on cybersecurity issues?							
monthly or more	41%	39%	52%	56%	44%	50%	43%
quarterly or more, but less frequently than monthly	29%	33%	30%	30%	32%	25%	36%
semiannually or more, but less frequently than quarterly	10%	9%	7%	3%	12%	17%	14%
yearly or more, but less frequently than semiannually	18%	18%	11%	11%	12%	8%	7%
less frequently than yearly	2%	1%	0%	0%	0%	0%	0%
never	1%	0%	0%	0%	0%	0%	0%
Do merger and acquisition proposals require a risk assessment from the team responsible for the issuer's cybersecurity?	78%	87%	78%	81%	86%	42%	83%
Does the issuer use multi-factor authentication (MFA) to manage remote access to internal resources, such as email?							
in all cases (96% - 100%)	71%	76%	78%	80%	80%	58%	79%
in most cases (66% - 95%)	20%	14%	20%	20%	16%	42%	14%
in about half the cases (36% - 65%)	4%	4%	1%	0%	4%	0%	0%
in a few cases (6% - 35%)	4%	5%	1%	0%	0%	0%	7%
no (0% - 5%)	2%	1%	0%	0%	0%	0%	0%

	Global	Global Banks	Global Healthcare	Global Healthcare Sectors			
				Not-for-profit hospitals	For-profit hospitals	Medical devices	Pharmaceuticals
Does the issuer have a program to track end-of-life (EOL) software?	85%	87%	90%	88%	96%	83%	92%
Does the issuer have a patch management policy?	95%	95%	100%	100%	100%	100%	100%
How often does the issuer backup its data and/or systems to a resource that is disconnected from the issuer's network?							
daily (or every few days)	81%	81%	89%	88%	95%	82%	90%
weekly (or every few weeks)	11%	14%	6%	6%	5%	9%	10%
monthly (or every few months)	4%	1%	2%	1%	0%	9%	0%
yearly (or less frequently than yearly)	3%	4%	3%	4%	0%	0%	0%
Does the issuer have a configuration management database (CMDB)?	80%	85%	82%	89%	63%	75%	85%
How often does the issuer conduct tabletop simulations?							
more than 4 times a year	7%	8%	6%	9%	0%	0%	7%
four times a year	5%	6%	10%	10%	12%	0%	14%
three times a year	3%	3%	4%	6%	0%	0%	7%
twice a year	15%	21%	24%	26%	16%	20%	29%
once a year	46%	52%	43%	37%	52%	70%	36%
every few years	10%	7%	6%	7%	8%	0%	0%
never	14%	2%	8%	6%	12%	10%	7%
How often does the issuer conduct penetration tests?							
more than 4 times a year	24%	49%	17%	19%	12%	8%	23%
four times a year	5%	6%	5%	6%	4%	0%	8%
three times a year	2%	1%	2%	0%	4%	0%	8%
twice a year	10%	9%	11%	13%	4%	8%	15%
once a year	46%	31%	58%	54%	64%	83%	46%
every few years	9%	3%	4%	4%	8%	0%	0%
never	4%	1%	3%	4%	4%	0%	0%
How often does the issuer conduct red team/purple team engagements?							
more than 4 times a year	9%	16%	4%	2%	4%	0%	17%
four times a year	2%	6%	2%	2%	0%	0%	8%
three times a year	1%	1%	2%	0%	0%	10%	8%
twice a year	6%	8%	7%	6%	4%	0%	25%
once a year	29%	37%	40%	44%	33%	50%	25%
every few years	15%	14%	10%	14%	0%	20%	0%
never	38%	18%	35%	33%	58%	20%	17%
Does the issuer have a program for responding to external reports of security issues affecting the company's products or operations?	56%	59%	59%	56%	58%	55%	79%
Does the issuer provide compensation for external reports of security issues affecting the company's products or operations?	18%	29%	11%	11%	14%	0%	20%
Do new vendors whose personnel or products have access to the issuer's computer systems require a risk assessment from the team responsible for the issuer's cybersecurity?							
in all cases (96% - 100%)	51%	62%	64%	68%	68%	42%	58%
in most cases (66% - 95%)	28%	22%	26%	25%	14%	50%	33%
in about half the cases (36% - 65%)	5%	1%	3%	3%	0%	0%	8%
in a few cases (6% - 35%)	9%	8%	5%	3%	9%	8%	0%
no (0% - 5%)	7%	6%	3%	2%	9%	0%	0%
Are the issuer's current vendors (whose personnel or products have access to the issuer's computer systems) subject to periodic review by the team responsible for the issuer's cybersecurity?							
in all cases (96% - 100%)	35%	48%	42%	40%	59%	18%	45%
in most cases (66% - 95%)	27%	25%	29%	31%	9%	55%	36%
in about half the cases (36% - 65%)	8%	8%	8%	11%	5%	0%	9%
in a few cases (6% - 35%)	19%	10%	17%	14%	23%	27%	9%
no (0% - 5%)	10%	8%	4%	5%	5%	0%	0%
Do contracts with vendors whose personnel or products have access to the issuer's computer systems require them to notify the issuer of cybersecurity incidents, vulnerabilities, patches, and/or malware that affect the vendors?							
in all cases (96% - 100%)	49%	62%	54%	57%	61%	27%	54%
in most cases (66% - 95%)	30%	22%	36%	36%	30%	36%	46%
in about half the cases (36% - 65%)	6%	4%	5%	3%	9%	18%	0%
in a few cases (6% - 35%)	9%	7%	2%	1%	0%	9%	0%
no (0% - 5%)	7%	6%	3%	3%	0%	9%	0%
Does the issuer require that vendors whose personnel or products have access to the issuer's computer systems carry cyber insurance?							
in all cases (96% - 100%)	18%	13%	37%	46%	30%	27%	14%
in most cases (66% - 95%)	19%	12%	32%	31%	43%	9%	36%
in about half the cases (36% - 65%)	6%	4%	3%	3%	0%	9%	0%
in a few cases (6% - 35%)	11%	18%	5%	5%	0%	18%	0%
no (0% - 5%)	46%	53%	24%	15%	26%	36%	50%

	Global	Global Banks	Global Healthcare	Global Healthcare Sectors			
				Not-for-profit hospitals	For-profit hospitals	Medical devices	Pharmaceuticals
RISK TRANSFER							
What percentage of the issuer's IT infrastructure is hosted on-premise (not on the cloud)?	65%	80%	75%	80%	70%	50%	30%
What percentage of the issuer's IT infrastructure is hosted on the private cloud?	5%	2%	10%	8%	5%	35%	16%
What percentage of the issuer's IT infrastructure is hosted on public cloud?	15%	5%	10%	7%	20%	25%	42%
What percentage of the issuer's IT infrastructure does it expect will be hosted on-premise (not on the cloud) 1 year from now?	50%	60%	65%	76%	30%	50%	21%
What percentage of the issuer's IT infrastructure does it expect will be hosted on the private cloud 1 year from now?	10%	4%	12%	10%	5%	35%	25%
What percentage of the issuer's IT infrastructure does it expect will be hosted on the public cloud 1 year from now?	20%	15%	15%	10%	20%	20%	45%
What percentage of the issuer's cloud assets fall under the infrastructure as a service (IAAS) model?	15%	6%	10%	5%	15%	25%	50%
What percentage of the issuer's cloud assets fall under the platform as a service (PAAS) model?	5%	5%	5%	3%	10%	10%	15%
What percentage of the issuer's cloud assets fall under the software as a service (SAAS) model?	30%	20%	35%	35%	20%	40%	41%
Does the issuer use more than one cloud provider?	46%	48%	50%	44%	54%	40%	77%
Does the issuer carry standalone cyber insurance?	75%	73%	95%	100%	83%	91%	93%
What insurance coverages are included in the issuer's standalone cyber policy?							
business interruption	77%	70%	76%	80%	71%	75%	67%
regulatory fines	57%	56%	67%	71%	76%	63%	33%
reputational damage	58%	50%	74%	73%	88%	75%	58%
contingent business interruption	56%	50%	70%	70%	71%	75%	67%
funds transfer fraud / business email compromise (BEC) / wire fraud	43%	35%	53%	59%	59%	38%	25%
incident response	77%	73%	81%	80%	94%	75%	67%
legal settlements	63%	57%	75%	80%	76%	63%	58%
new equipment	43%	35%	51%	55%	41%	38%	50%
property damage	39%	47%	42%	46%	29%	25%	50%
ransom payments	72%	64%	81%	82%	100%	75%	50%
What is the percentage change in your standalone cyber insurance premium between 2020 and 2022?	49%	31%	73%	75%	48%	109%	94%
Does the issuer expect to buy more, the same or less cyber coverage in 2023?							
about the same	81%	77%	82%	83%	74%	100%	73%
more	16%	21%	17%	17%	21%	0%	27%
less	3%	3%	1%	0%	5%	0%	0%
Does the issuer have explicit cyber coverage through a traditional insurance policy?	38%	41%	46%	54%	33%	63%	21%
What cyber coverages are explicitly included in the issuer's traditional insurance policy?							
business interruption	58%	49%	73%	73%	71%	75%	75%
regulatory fines	36%	39%	44%	58%	14%	25%	25%
reputational damage	38%	43%	49%	54%	29%	25%	75%
contingent business interruption	42%	35%	59%	58%	57%	50%	75%
funds transfer fraud / business email compromise (BEC) / wire fraud	40%	55%	49%	46%	43%	75%	50%
incident response	44%	43%	51%	62%	29%	25%	50%
legal settlements	40%	51%	46%	58%	29%	25%	25%
new equipment	33%	27%	44%	54%	29%	25%	25%
property damage	53%	57%	66%	65%	43%	100%	75%
ransom payments	42%	39%	46%	58%	29%	25%	25%
DISCLOSURES							
Does the issuer have any cyber incident reporting requirements for incidents that do not result in the disclosure of personally identifiable information (PII)?	66%	92%	67%	63%	64%	80%	85%
Has the issuer ever issued a public notice of a cyber incident?	22%	24%	34%	42%	32%	18%	7%
Has the issuer reported any cybersecurity incidents it has experienced to regulators over the past 2 years?	27%	49%	28%	29%	24%	30%	31%
Has the issuer reported any cybersecurity incidents to its customers over the past 2 years?	21%	19%	27%	30%	26%	27%	14%
Has the issuer reported any cybersecurity incidents to its board/council over the past 2 years?	46%	58%	50%	44%	46%	64%	77%

Source: Moody's Ratings

REPORT NUMBER 1396317

CLIENT SERVICES

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