SECTOR IN-DEPTH
17 June 2024

Send Your Feedback

Contacts

Chris Scott +49.69.86790.2131
AVP-Analyst
chris.scott@moodys.com

Luca Brusadin +49.69.70730.877
Ratings Associate
luca.brusadin@moodys.com

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

Karen Berckmann, CFA +49.69.70730.930
Associate Managing Director
karen.berckmann@moodys.com

CLIENT SERVICES

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

Chemicals – Global

2023 Cyber Survey - Chemical firms step up cyber risk preparedness as new rules loom

Summary

Awareness of cybersecurity vulnerabilities is rising in the chemicals industry, according to a survey of the chemical firms we rate around the globe[1]. Our 2023 cyber survey shows chemical companies have increased their cyber budgets after an escalating number of incidents and as new regulations loom. The chemical industry is at high risk in the event of a cyberattack because the impact can ripple downstream, affecting the supply of key inputs for industries including auto, construction, medical applications, and water purification.

Chemical companies have boosted cyber budgets; management awareness of cyber risks has risen. Over the last five years, nearly all respondents from the chemicals industry said they have alloted the same amount or more of their IT budgets toward cybersecurity. Small and mid-sized firms are leading the pack with total cyber spending at around 10% of the IT budget. Many firms said they have established direct cyber-related reporting lines to the board of directors and have ensured cybersecurity knowledge exists on the board itself.

Heightened awareness comes as new regulatory requirements loom. EU and US regulators have increased their focus on cybersecurity for mission-critical sectors of the economy. Both jurisdictions have established new laws and mandates for these sectors that will likely include many chemical firms. The new requirements are expected to go live in the EU in October 2024 and for the final rules to be issued in October 2025 in the US.

Basic cyber defense practices are near universal; advanced strategies found in larger firms. Chemical companies are displaying greater sophistication in their cyber defense strategies, using a mix of basic and advanced methods. The survey shows good implementation of basic strategies, while more advanced and costly practices are still skewed toward larger companies.

Firms in the Americas have stricter cybersecurity requirements for external software providers; higher incident reporting to regulators for large issuers. Third-party software poses a significant risk for corporations. Chemical companies often neglect periodic assessments of the cyber practices of these providers. Separately, incident reporting to boards and regulators is increasing, highlighting a trend towards greater transparency.

Cyber insurance is more prevalent in Americas and EMEA. About 70% of chemical industry respondents carry standalone cyber insurance. Standalone coverage was most common in the Americas (88%), followed by EMEA (60%). In APAC no responding issuers were carrying cyber insurance.

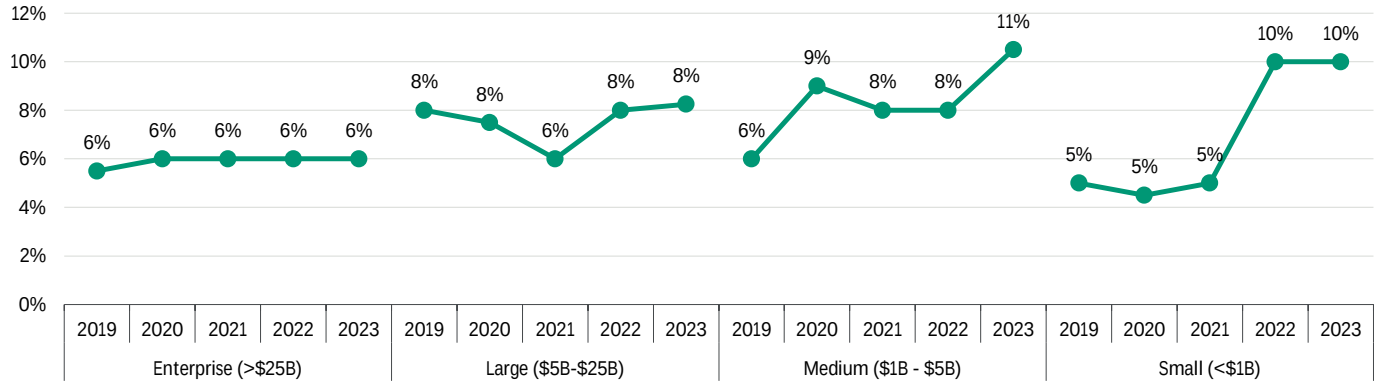
Chemical companies have boosted cyber budgets; management awareness of cyber risks has risen

Over the last five years, nearly all chemical companies who responded to our 2023 global cyber survey said they have allocated the same amount or more of their IT budgets toward cybersecurity. While our cohort of large and enterprise-sized issuers have seen their budgets for cyber-related spending remain flat (on a % basis), small and mid-size companies have been increasing their allocation to cyber defense. This likely represents a catch-up from historical underinvestment, and also reflects the fact that smaller companies must invest a higher percentage of their budgets to maintain a minimum standard of defense.

Exhibit 1

Smaller companies are playing catch-up

Percentage of total technology budget allocated to cybersecurity



2023 figures are the companies' projections

Source: Moody's Ratings

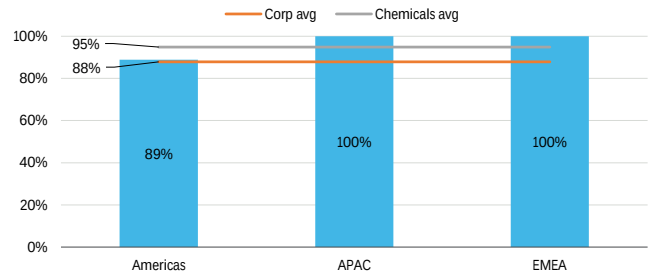
Companies have also established direct cyber reporting lines to the board of directors, tied CEO compensation to cyber risk performance, and ensured cybersecurity knowledge exists on the board itself.

A key indicator of cyber governance is the proximity of the Chief Information Security Officer (CISO) to the executive team. A close reporting structure can foster greater cybersecurity awareness and thereby garner better support for enterprise-wide cyber risk management. The survey findings show that, globally, 88% of corporate cybersecurity heads report directly to a C-suite executive (Exhibit 2). This figure is even higher in the chemical sector at 95%, indicating a strong governance structure supporting cybersecurity threats awareness among top-tier executives. Reporting frequency is also regular with 44% of chemical issuers reporting at least monthly to the CEO. This is slightly better than the 40% for our entire global corporate universe (Exhibit 3).

Exhibit 2

Head of cyber reports directly to C-suite at most chemical issuers

% reporting directly to C-suite

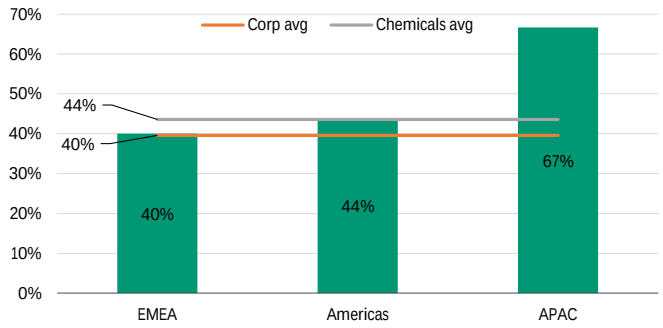


Source: Moody's Ratings

Exhibit 3

APAC leads in frequency of reporting to the CEO

% senior cyber manager reporting at least monthly to the chief executive



Source: Moody's Ratings

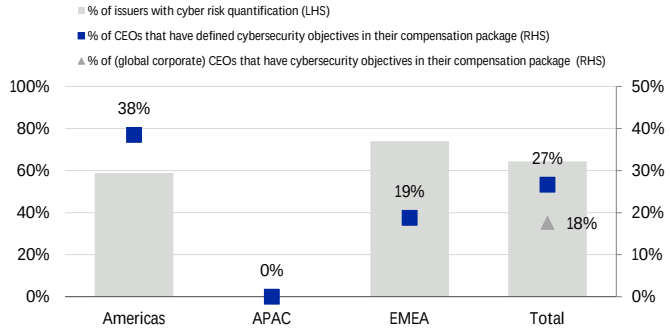
The survey reveals a noteworthy trend in the Americas, where 38% of respondents reported that their CEOs' compensation is linked with cybersecurity objectives. This figure is significantly higher than the average of 27% globally for chemical companies, and contrasts with the APAC region where such linkage is not prevalent (Exhibit 4). The 27% of chemicals sector respondents which link compensation to cyber objectives, is much higher than the 18% observed on a global corporate basis. This suggests a strategic prioritization of cybersecurity in the Americas and in the chemicals industry, which could be a factor in their robust cyber risk management practices.

In terms of cyber risk quantification practices, where risk managers financially quantify their cyber risk exposure and develop data-driven mitigation plans, the EMEA and Americas regions demonstrate robust methods. In the APAC region, however, such practices were absent among responding issuers (Exhibit 4). Furthermore, the survey indicates that the largest companies tend to have above-average cyber expertise within their board of directors. On average 16% of chemical firms have cyber expertise on the board, which is in line with the global corporate average, but higher than our global average across all sectors at roughly 10%. However, this expertise is not observed among small chemical issuers (Exhibit 5).

Exhibit 4

CEO compensation is increasingly tied to cybersecurity

% of issuers with cyber risk quantification and % of respondents with CEO compensation tied to cybersecurity



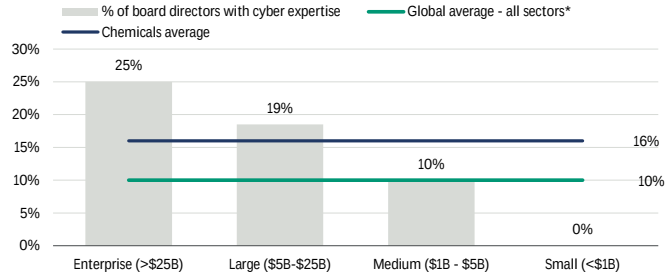
Cyber risk quantification means the issuer assesses cyber risk in terms of financial impact

Source: Moody's Ratings

Exhibit 5

Chemicals firms have above-average board expertise on cybersecurity, with larger companies at the forefront

% of respondents with cyber expertise on their boards



*Global average of our survey respondents across all sectors (corporate, infrastructure, financial institutions)

Source: Moody's Ratings

Heightened awareness comes as new rules loom

Since our last survey in 2020, many cyber preparedness indicators have shown noticeable improvement. Firms are keenly aware of potential financial costs and reputational damage related to cyber incidents - events which act as a key preparedness motivators. But there is also an ongoing push by regulators to drive companies to make cyber defense a higher priority. Two notable pieces of regulation in the US and the European Union (EU) will likely bring additional focus to cybersecurity over the next 18 months.

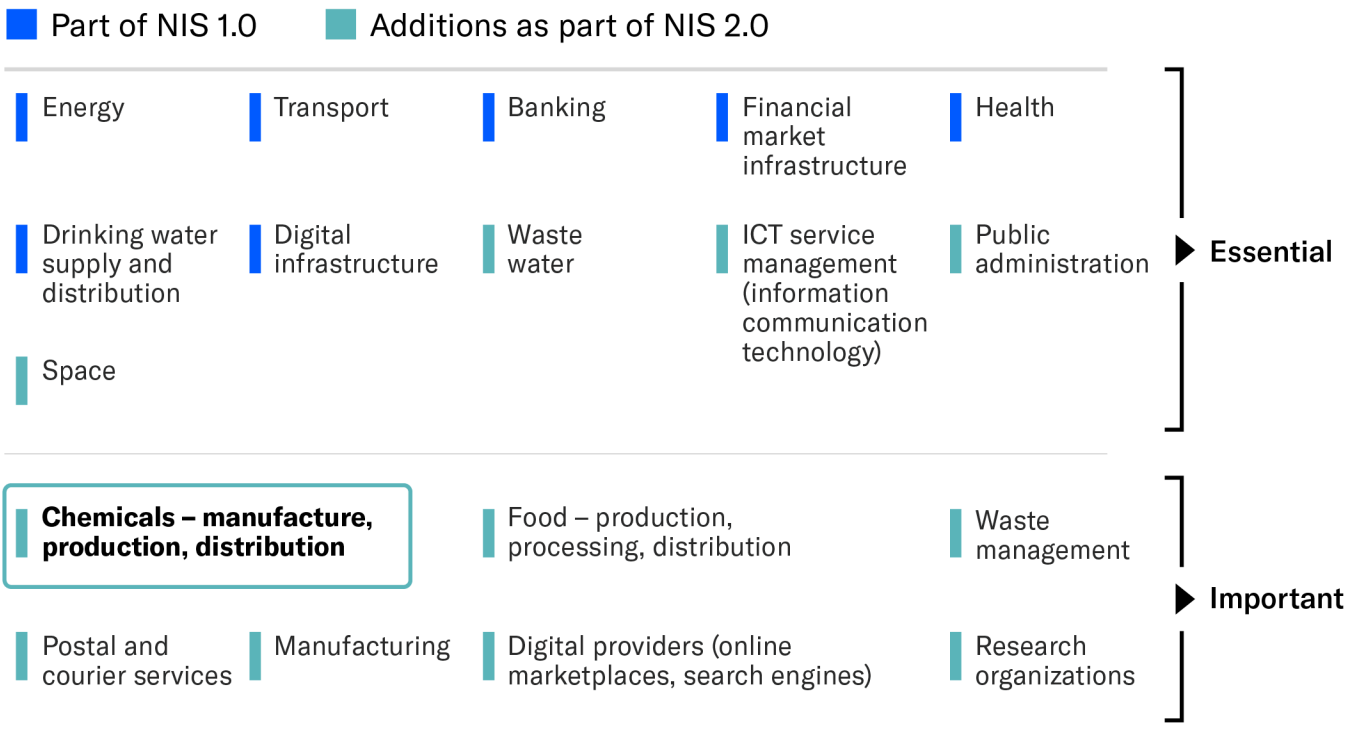
In March 2022, the US signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA mandates the Cybersecurity and Infrastructure Security Agency (CISA) to create rules for certain mission-critical companies to report cyber incidents and ransom payments. This allows CISA to promptly allocate resources to help attack victims, identify patterns from reported incidents and swiftly share this data with network defenders to alert potential targets. On April 4, 2024, CISA published a Notice of Proposed Rulemaking (NPRM) and expects the final rules to be issued in October 2025, potentially taking effect in early 2026.

CISA is proposing to defining covered entities (covered entity FAQ) as those of sufficient size (based on number of employees or annual revenue) as well as those that meet specific sector-based criteria.

It is likely that many chemical companies will be captured under CIRCIA's scope. The criteria include entities "in a critical infrastructure sector, as defined in Presidential Policy Directive". The PPD does not include a definition for "critical infrastructure sector," but it does provide a list of the 16 critical infrastructure sectors - of which chemicals is one. Additionally, companies which own or operate a chemical facility covered by CFATS (Chemical Facility Anti-Terrorism Standards) [2]would be in-scope for CIRCIA.

In January 2023, the EU passed a new version of its Network and Information Security (NIS) Directive, NIS 2.0. NIS 2.0 brings into scope more industries and imposes cyber risk management, incident reporting and information-sharing obligations on certain types of organizations (deemed important and essential) in a range of sectors. EU member states will need to adopt and publish the measures necessary to comply with NIS 2.0 by Oct. 17, 2024. Within the EU, most if not all, chemical-related firms are likely to be categorized as "important" under the new legislation (Exhibit 6), given the broad language used in the legislation.

Exhibit 6
NIS 2.0 directive broadens industries covered and enhances overall cyber resilience and awareness
Industries deemed either "essential" or "important"



These entities are deemed to be under the jurisdiction of the EU country where they are established. If the entity is established in more than one member state, it will fall under the jurisdiction of both.
Sources: European Union and Moody's Ratings

We view these legislative developments as credit positive for the sector as the entirety of the chemicals supply chain and related upstream and downstream industries will have greater cyber protection and resilience.

Basic defense practices are near universal; advanced strategies found in larger firms

Chemical issuers exhibit a high degree of sophistication in their cyber defense strategies, using a mix of basic and advanced methods. Our survey data reveal that basic strategies are substantively implemented. Incident response plans are the most prevalent, boasting nearly universal adoption across all regions. Multifactor authentication for remote access into networks was slightly less robust, at close to 90% for chemical firms (Exhibit 7). Furthermore, chemical issuers reported more frequent use of cyber assessments during merger and acquisition due-diligence procedures, at 82% compared with 79% for all of our responding corporate finance issuers.

Below is a summary of the basic cyber defense practices we asked about:

» **Incident response plans and testing** are the foundation of cyber risk management. All chemical survey respondents say they have implemented such plans. Incident response plans are most effective when they are regularly tested, reviewed and updated. 91% of our surveyed companies said they update their plan once a year or more frequently.

» **Weekly data backups** to a system that is disconnected from an organization's network is an effective way to rapidly restore operations after a ransomware attack. These attacks typically encrypt the target's files, hampering or halting operations until a ransom key is provided by the attacker, or a company is able to successfully restore its systems via its backups.

» **Multifactor authentication** to manage remote access is used by 89% of survey respondents and is increasingly important in light of rapid and wide adoption of remote-work arrangements. This compares favorably with all corporate issuers where adoption is 72%.

» **Cyber risk assessments of acquisition targets** are a requirement at many chemical companies, but more common at larger ones.

Exhibit 7

Basic defense tactics are nearly universal but there are some gaps

	Global corporate avg	Chemicals avg	Americas	APAC	EMEA
% that have an Incident Response Plan	97%	95%	100%	100%	90%
% that back up data and systems daily (or every few days)	81%	84%	100%	100%	71%
% that use multifactor authentication for remote access to internal resources	72%	89%	94%	100%	86%
% that require cyber risk assessments of M&A targets	79%	82%	92%	100%	73%

Source: Moody's Ratings

Below is a summary of advanced cyber defense practices (Exhibit 8) we asked about:

» **Tabletop exercises** are role-playing activities where participants respond to scenarios. These are important for evaluating an organization's cyber risk processes, tools, and proficiency in responding to different attack scenarios. Some 19% of our survey respondents never carry out tabletop exercises to practice strategic and technical responses to a cyber event.

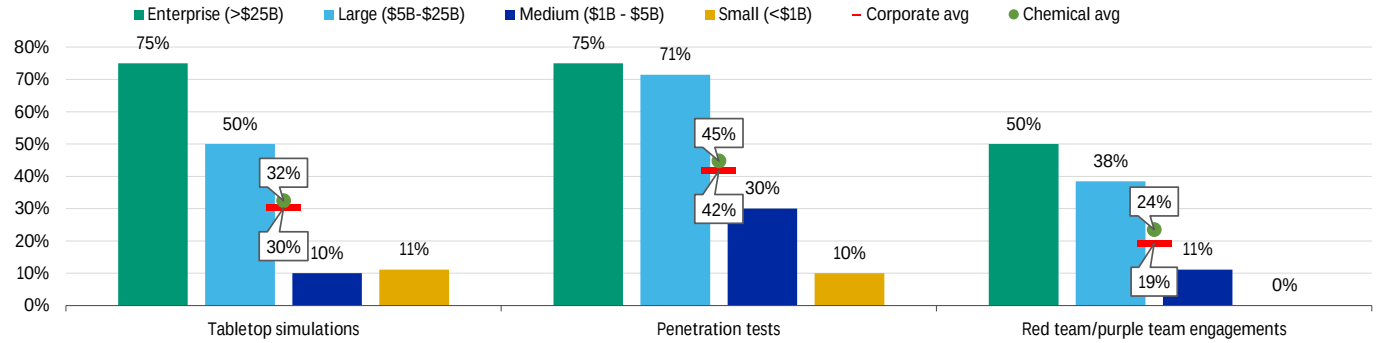
» **Penetration tests** are a simulated attack using the same tools, techniques and processes as malicious hackers to expose weaknesses in computer systems, networks and applications. The goal of these tests is to identify as many vulnerabilities as possible. This was the most common test among our survey respondents, with 95% saying they conducted these tests at least every few years. Only 45% of chemical issuers are conducting penetration tests more than once a year. This compares less favorably with the 58% in the technology industry, but is more frequent than the oil and gas and steel industries, where only 28% and 22% of respondents indicated they conducted penetration tests more than once a year.

» **Red/purple team engagements** are long-term continuous assessments that mimic real-life attackers. Red teams take the role of hackers and try to uncover security vulnerabilities. Purple teams, a cooperative effort between Red (offensive) and Blue (defensive) teams, focus on shared learning and improved defenses from discovered offensive strategies, bolstering security measures proactively. The goal is to test an organization's detection and response capabilities. The test is often kept secret from parts of the security team. Around 35% of our chemical survey respondents have never conducted Red/Purple team engagements, while 24% say they are conducting them more than twice a year.

Exhibit 8

Advanced defense tactics are limited to the largest issuers

Chemical issuers with at least two tests per year, by size



Source: Moody's Ratings

Overall most of the advanced tactics were practiced more often by our larger issuers as they can be more costly and more complicated to administer.

The Americas have stricter cybersecurity requirements for external software providers

Even as companies bolster their cybersecurity measures, third-party software providers remain a potential weak link, especially among chemical firms, which showed lower standards than global companies (Exhibit 9). However fortified a company's internal IT infrastructure is, it may still be susceptible to breaches originating from external vendors granted access to its systems, whose security has been compromised.

The distribution of companies imposing additional cyber protection measures on vendors varies materially across regions. The Americas have the most stringent requirements. Issuers in the Americas have a greater frequency of new vendor assessments (79%) and more often require timely notification of cyberattacks affecting vendors (91%), compared with just 50% and 61% in EMEA respectively. While not a majority, 42% of companies in the Americas require third-party vendors to carry cyber insurance while only 12% of EMEA companies require the same standard. Chemical firms in the Americas are also more likely to require ongoing vendor assessments. This implies a greater focus on third parties as a potential cyber risk in the Americas. Similar measures are yet to become commonplace in other regions.

Exhibit 9

The Americas lead in standards for screening new third-party software vendors

Cyber risk practices for third-party supplier relationships by region

	Global corporate avg	Chemicals avg	Americas	APAC	EMEA
% that require cyber risk assessment of new vendors	75%	65%	79%	100%	50%
% that require periodic cyber risk assessments of current vendors	56%	40%	50%	100%	27%
% that receive timely notification of cybersecurity incidents and vulnerabilities that affect vendors	75%	73%	91%	100%	61%
% that require vendors to carry cyber insurance	32%	24%	42%	0%	12%

Percentages represent respondents that require these checks for more than 66% of their vendors
There was just one respondent to these questions in the APAC region.
Source: Moody's Ratings

Exhibit 10 below shows that the largest chemical companies require stricter cyber practices from new software vendors, as well as a timely notification from third-party vendors on cybersecurity incidents. Small issuers, however, have not imposed these requirements, whether due to lack of knowledge of these practices or less power when negotiating commercial terms with suppliers. The number of issuers that require periodic assessments on current vendors is weak across chemical issuers regardless of size.

Exhibit 10

Enterprises holds stricter cybersecurity standards for external providers

Cyber risk practices for third-party software supplier relationships by company size

	Enterprise	Large	Medium	Small
% that require cyber risk assessment of new vendors	100%	73%	64%	20%
% that require periodic cyber risk assessments of current vendors	50%	30%	55%	20%
% that receive timely notification of cybersecurity incidents and vulnerabilities that affect vendors	100%	89%	75%	44%
% that require vendors to carry cyber insurance	67%	30%	14%	11%

Percentages represent respondents that require these checks for more than 66% of their vendors

Source: Moody's Ratings

Larger entities are more likely to report cyber incidents to various stakeholders

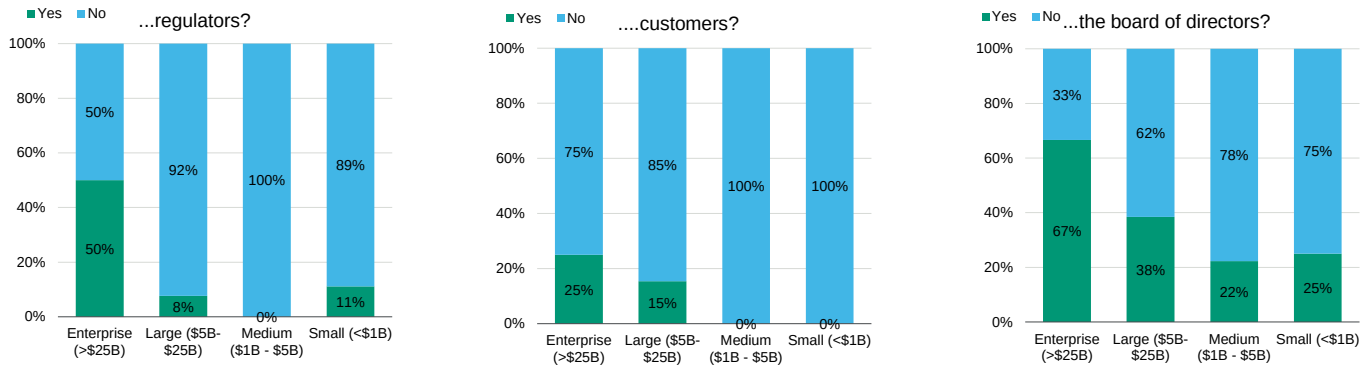
The practice of reporting cyberattacks to the board of directors is gaining traction among companies, particularly among larger enterprises. This trend underscores the heightened reporting standards within these organizations, where cyber managers more actively engage in the assessment and communication of cyber incidents with top-tier executives.

Survey results further reveal more frequent reporting of cyberattacks to regulators by the largest chemical firms (Exhibit 11), potentially due to the firms strategic importance for the economy and society, with half of all incidents being reported. Additionally, the US Securities and Exchange Commission imposes specific disclosure requirements on publicly listed companies. We expect the CIRCIA and NIS 2.0 regulations to result in increased reporting, both internally (to boards of directors) and for external stakeholders like regulators and customers.

Exhibit 11

Reporting frequency is skewed toward larger entities

We asked: in the past 24 months, has your organization reported any cybersecurity incidents to...



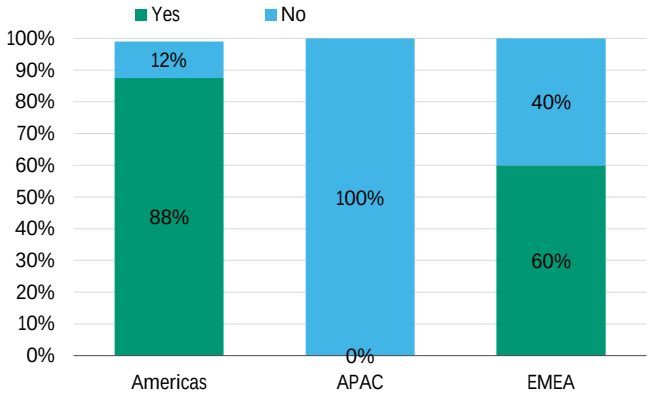
Source: Moody's Ratings

Stand-alone cyber insurance is more prevalent in Americas and EMEA; APAC expects to increase coverage

About 70% of respondents said they carry stand-alone cyber insurance. Coverage was most common in the Americas (88%), followed by EMEA (60%). While none of our responding issuers from APAC indicated they currently carried cyber insurance, all of them said they intend to purchase it this year (Exhibit 13).

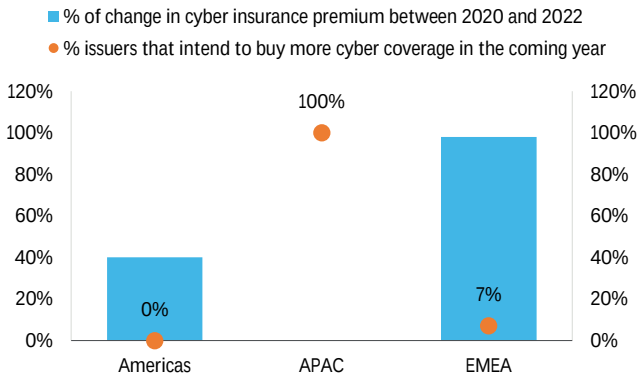
Many of our rated chemical issuers cited exorbitant insurance premiums as one reason for not purchasing standalone cyber insurance, instead choosing to self-insure. According to reinsurer Swiss Re, cyber insurers raised their cyber insurance rates significantly in 2021 and 2022 to restore profitability after a rise in ransomware attacks led to heavy losses in preceding years. In 2023, Swiss Re observed that rates had stabilized and insurers had become more selective with their pricing for specific segments of the market. Willis Towers Watson, an insurance broker, noted in its spring 2024 market update, that premium stabilization has continued with flat rates for renewals and in some instances even decreases. Increases, if any, are typically seen by those organizations that cannot demonstrate strong ransomware controls. We expect this price stabilization could lead more issuers to purchase cyber insurance in coming years.

Exhibit 12
Cyber insurance is less prominent in APAC
% of global respondents with standalone cyber insurance



Source: Moody's Ratings

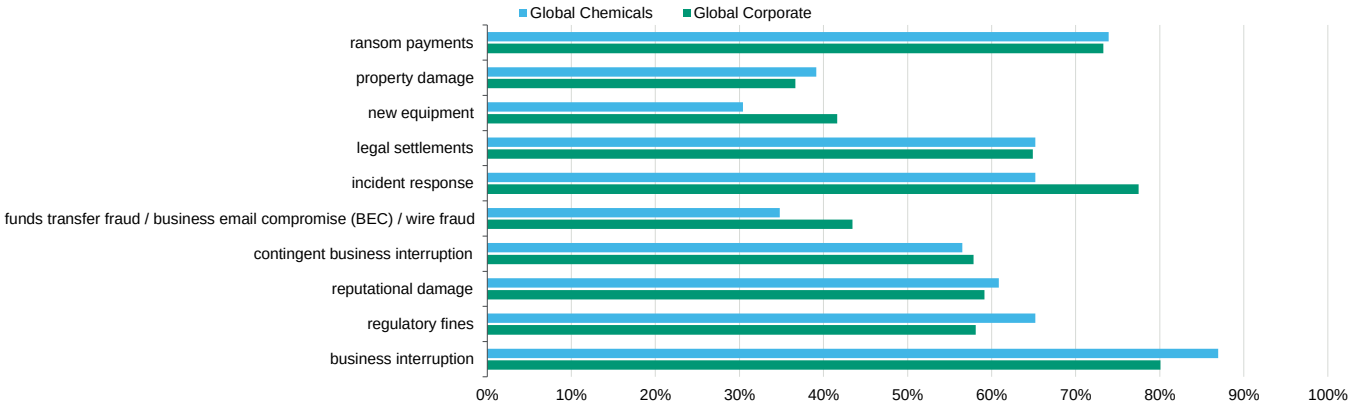
Exhibit 13
100% of APAC issuers intend to buy more coverage



Source: Moody's Ratings

Then exhibit below shows the different cyber incidents covered by our respondents' cyber insurance policies. The most common incidents covered include business interruption, ransom payments, reputational damage, legal settlements, regulatory fines and incident response. This aligns closely with the responses of companies across all nonfinancial corporate sectors.

Exhibit 14
Chemicals firms carry similar levels of cyber insurance coverage as firms across the corporate spectrum
Percentage of issuers with specific coverage terms under cyber policies



Source: Moody's Ratings

About our cybersecurity survey

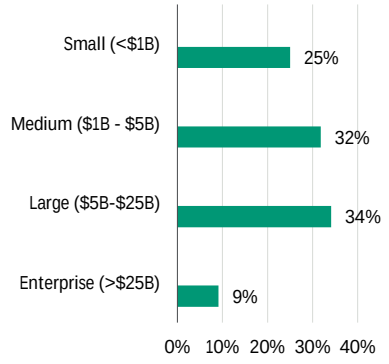
This report presents the findings from a global corporate cybersecurity risk survey. The survey encompasses 44 issuers under the chemicals methodology that collectively comprise around 29% of the total number of rated issuers under the chemical methodology.

The survey, involving around 90 questions, investigated enterprise cybersecurity strategies, IT infrastructure, third-party vendor management, insurance, cybersecurity expenditure and corporate governance. Nonetheless, this report primarily focuses on elucidating the key findings derived from the responses, not encompassing a comprehensive discussion of all posed questions.

The data from respondents has been grouped by size and regions: Americas; Europe, the Middle East and Africa (EMEA); and Asia-Pacific (APAC). Our survey provides a robust benchmark for how companies in the chemical sector structure their cyber risk governance, management and risk transfer policies. Exhibits 15 to 17 display the respondent profiles by size, region and rating level.

Exhibit 15

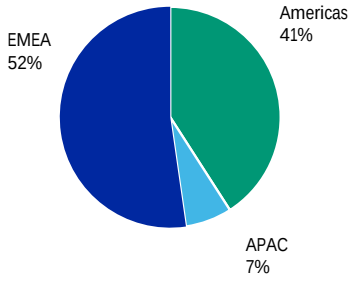
Survey respondents by size



Source: Moody's Ratings

Exhibit 16

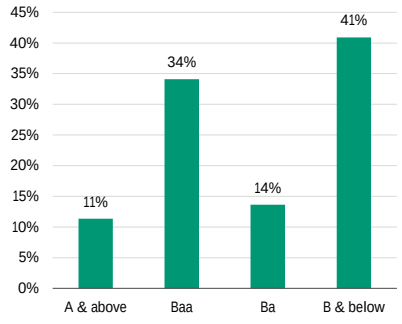
Survey respondents by region



Source: Moody's Ratings

Exhibit 17

Survey respondents by rating



Source: Moody's Ratings

Endnotes

1 Moody's 90-question survey of more than 1,900 respondents gauged cybersecurity practices among global debt issuers and collected data on an emerging risk that carries the potential to influence the credit profile of all debt issuers. This report focuses on the responses of issuers in the chemicals sector.

2 CFATS is a regulatory program in the US that identifies and regulates high-risk facilities that possess certain chemicals of interest at specific concentrations and quantities. As of July 28, 2023, Congress allowed the statutory authority for the Chemical Facility Anti-Terrorism Standards (CFATS) program to expire. Therefore some combination the PPD and CFATS criteria are expected to be used.

REPORT NUMBER 1383401

CLIENT SERVICES

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