MOODY'S INVESTORS SERVICE

SPECIAL SERIES Global Cyber Risk Issuer Surveys

SECTOR IN-DEPTH
24 April 2024

Send Your Feedback

TABLE OF CONTENTS

Contacts

Melissa Nicandri +1.212.553.3890
Associate Lead Analyst
melissa.nicandri@moodys.com

Heather Correia +1.214.979.6868
AVP-Analyst
heather.correia@moodys.com

Orlie Prince +1.212.553.7738
Senior Vice President/Manager
orlie.prince@moodys.com

Emily Raimes +1.212.553.7203
Associate Managing Director
emily.raimes@moodys.com

CLIENT SERVICES

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

Higher Education – Global

Cybersecurity planning prioritized across sector but smaller institutions play catch-up

Summary

Colleges and universities are allocating a growing share of their budgets to cyber spending, according to our latest cyber survey, underscoring an increasing focus on cyber risk. But while most institutions conduct long-term cybersecurity planning, smaller, less well-resourced issuers trail both their peers and global averages in adopting multiyear road maps and incident response plans. Standalone cyber insurance remains common among most issuers despite a sharp rise in premiums. Across the sector, employees are increasingly discussing cyber risk with upper management, though larger, richer institutions are more likely to have dedicated cyber staff. The observations in this report reflect survey responses and do not represent a definitive assessment of cybersecurity readiness.

» **Spending on cybersecurity has risen over the past five years.** The share of budgets allocated to cybersecurity rose by 73% between 2019 and 2023 for all respondents. The increase was even larger for lower-rated institutions, which are likely playing catch-up and trying to upgrade their systems to protect against the risk of cyberattacks.

» **Cyber planning now a priority, but fundamental cyber defense frameworks are not universal across small institutions.** About 95% of issuers have an incident response plan (IRP), and 86% engage in multiyear cyber planning. The smallest institutions trail global averages, however, with only 83% having an IRP and 75% a multiyear road map.

» **Public universities in the US are more likely to report cyber incidents given stronger disclosure requirements.** Disclosure varies by type of institution, with public universities subject to more stringent, government-imposed reporting requirements.

» **Most issuers carry standalone cyber insurance, with the largest more likely to buy additional coverage.** Despite a 111% rise in premiums, the share of respondents with standalone policies has not materially changed since the 2021 survey and remains high. About 30% of larger, well-resourced institutions indicated they would buy more coverage in 2023, but small and medium-sized institutions said they would hold steady.

» **Larger institutions have more dedicated cyber staff and are more likely to report to the board or president.** Though not all institutions have the resources for dedicated cyber staff, communication on cybersecurity is growing, with many issuers having monthly or quarterly conversations with the board or president. Still, smaller issuers remain weak on some basic cyber governance practices.

Our latest survey of cyber risk preparedness among global and US higher education institutions covered a range of topics, from governance to operations to risk transfer. We asked universities and colleges about their hiring of cybersecurity employees, use of advanced cybersecurity defenses, management of cybersecurity concerns in their supply chains and among third-party vendors, and their cyber insurance coverage.

We received 114 responses from universities and colleges. Respondents were mostly US-based institutions, but we also received feedback from organizations in Europe and Asia-Pacific. Of the 114 surveys received, respondents included 46 US public universities, 48 US private universities, and 20 public international universities. Moody's last cyber survey was circulated in 2021 and had 32 respondents. To analyze the data, we considered several factors, including geographic location, rating category, type of institution (e.g. public or private) and size. We defined size based on total cash and investments, with the breakout shown in Exhibit 1.

Exhibit 1

Total cash and investments	Size category
< $250 million	Small
$250 million - $1 billion	Medium
$1 billion - $5 billion	Large
> $5 billion	Extra large

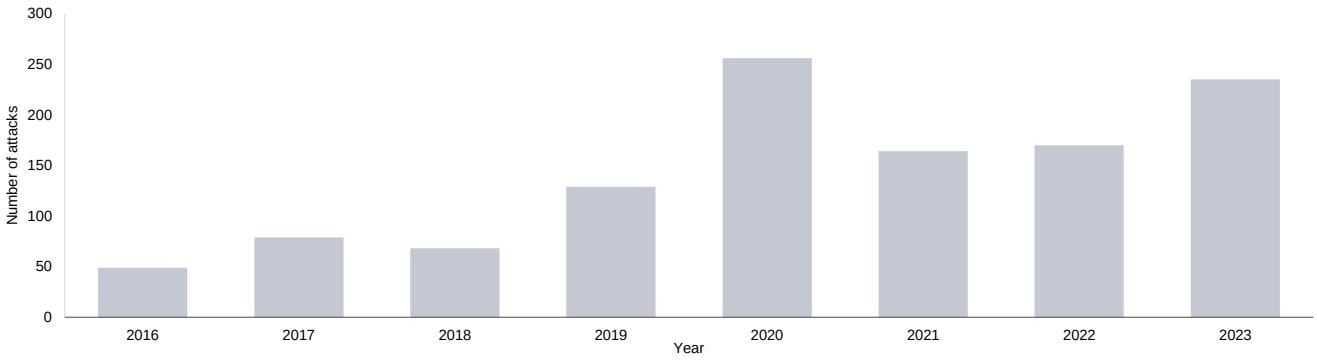
Source: Moody's Ratings

Spending on cybersecurity has risen over the past five years

Over the past five years, spending on cybersecurity has risen among all higher education institutions. Universities and colleges are particularly vulnerable to cyberattack because of a high concentration of personal student and faculty data. As attacks on the sector have grown in the past eight years (see Exhibit 2). The University of Maryland estimates that the frequency of cyberattacks in the education services industry has grown by 34% per year on average, and institutions have increased their spending on cyber to protect their data and reputation. Institutions that operate research or academic medical centers are at greater risk of attack given the presence of sensitive personal and financial data. Favorably, these types of university systems also tend to be well resourced and staffed, providing somewhat of a mitigant to criminal activity. Generally, the portion of budget allocated to cybersecurity has grown, on average, about one percentage point each year. In 2023, the sector average was 7%, similar to other public finance sectors, but slightly below the global average of 8%.

Exhibit 2

Cyberattacks on the educational services sector have risen in the past eight years



*Data set includes some K-12 schools.

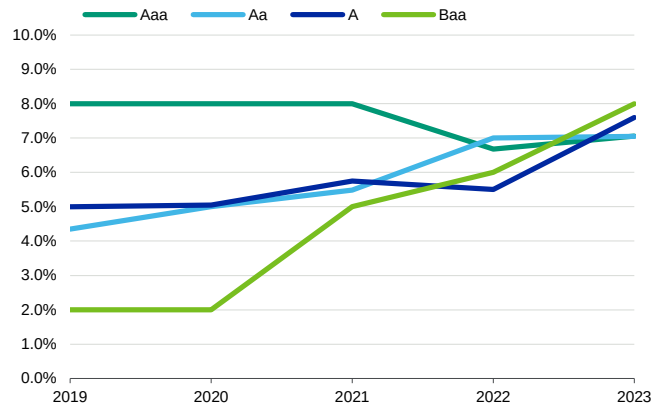
Source: University of Maryland CISSM Cyber Attacks Database, Harry, C., & Gallagher, N. (2018). Classifying cyber events. Journal of Information Warfare, 17(3), 17-31

The pace at which cyber spending has risen varies across size and rating categories. Increases in cyber budgets have been larger among lower-rated issuers as they play catch-up to higher-rated institutions (see Exhibit 3), which over the years have enjoyed more resources to build out their cyber practices and buy insurance. A similar difference on cyber spending exists between large and small institutions (see Exhibit 4). When it comes to dedicating a line item for cybersecurity in their budgets – an indicate that an organization recognizes that cyber risk is here to stay – only 31% of small institutions indicated they did so compared to 91% and 84% of extra large and large institutions, respectively.

Exhibit 3

Baa-rated issuers had the biggest increases in their cyber budgets between 2019 and 2023

Cyber investment as a % of IT budget

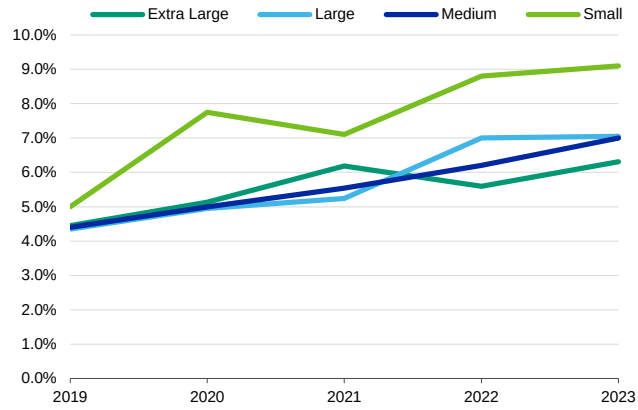


Source: Moody's Ratings

Exhibit 4

By size, smaller issuers saw the greatest budget growth

Cyber investment as a % of IT budget



Source: Moody's Ratings

On a nominal basis, spending on cybersecurity between 2019 and 2023 climbed 73% among higher education issuers globally. The most significant jumps in spending occurred for Baa-rated and small issuers, with 104% and 100% increases respectively. Given the steady rise in cyber insurance premiums, it is likely that a good portion of that increase was to maintain existing plans.

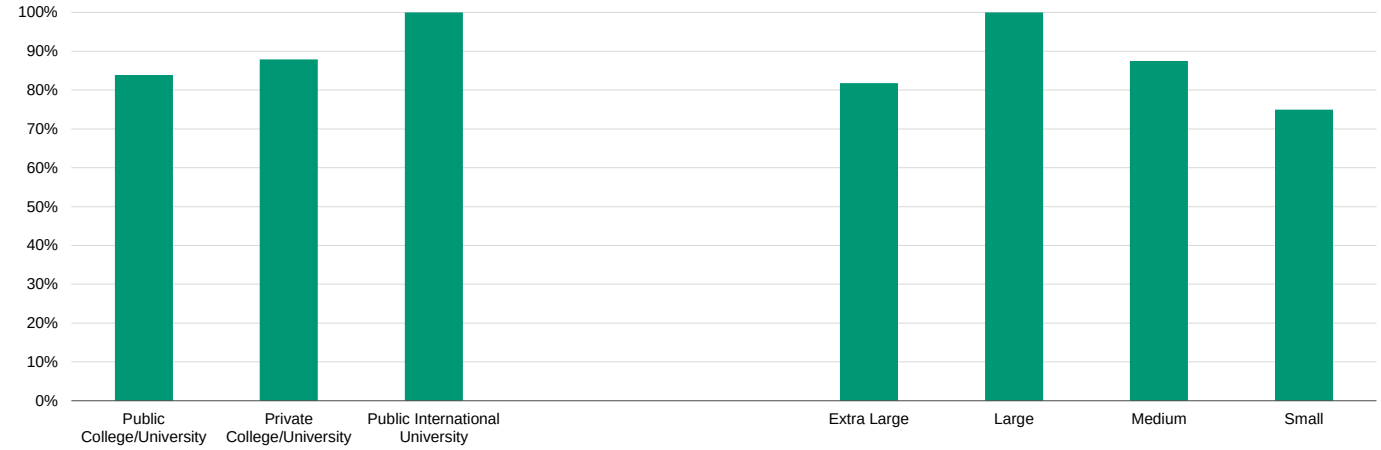
Small issuers trail in incident response and longer-term cyber planning

Awareness of cyber risk among higher education institutions is high overall. Over 95% of extra large, large and medium sized institutions have a cyber incident response plan (IRP). Further, 100% of that same set of respondents participate in industry threat information sharing groups. Smaller institutions trail their larger peers, however, with only 83% indicating they have an IRP and 74% participating in industry sharing.

When it comes to longer-term planning, 100% of international university respondents have a multiyear cybersecurity road map, ahead of US publics and privates with 84% and 88%, respectively. Digging into the data, this is another area where our smallest issuers lag: only 75% of respondents stated they had a multiyear road map (see Exhibit 5). US higher education institutions are facing headwinds, such as declining enrollment trends, which directly impacts revenues. Smaller institutions have fewer resources, and thus, less financial flexibility, to address these challenges and may choose to focus on facilities or academic programming rather than their cyber stance.

Exhibit 5

All international university respondents have a multiyear cyber road map, an area where small US issuers lag



Source: Moody's Ratings

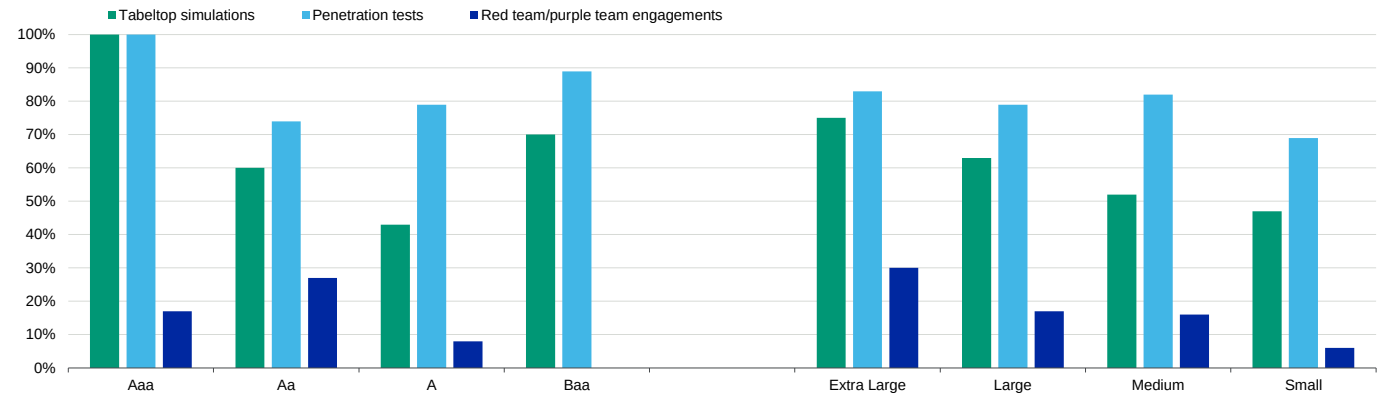
While presence of an IRP indicates awareness of cyber risk, equally important is the frequency of testing: testing of an established IRP ensures an issuer is prepared to effectively respond to an attack. Our data indicates that, on average, around 51% of the sector tests their IRPs once per year. This is roughly in line with the global average of 53%. However, a portion of large (8%), medium (14%) and small (13%) institutions reported that they never tested their IRP, which is a weakness. Similarly, on average, 59% of the sector reviews and updates their IRP once per year (aligned with the global average of 59%), but the data shows that 6% of our small issuers never engage in this practice.

About 78% of issuers in total conduct a penetration test – a simulated cyberattack to evaluate a computer system's security – at least once a year, with higher-rated and extra-large issuers most likely to do so. In the Aaa category, for example, 100% of respondents conduct penetration tests at least once a year.

Generally, larger and higher-rated institutions test their systems more frequently than lower-rated issuers (see Exhibit 6), though among Baa-rated respondents about 90% performed penetration tests at least annually. This is a significant change from the 2021 survey, when only 5% of public and 10% of private institutions indicated use of penetration testing.

Exhibit 6

Larger and higher-rated institutions test their systems more frequently than lower-rated issuers, with penetration tests most common



Source: Moody's Ratings

The type of testing done also varies. Penetration tests are most common, while red team/purple team testing is conducted very infrequently. The latter is a more targeted form of penetration testing that typically involves an internal and external team that uses real-life attacker tactics to test an organization's physical and cybersecurity defenses. Such testing tends to be very expensive, and is

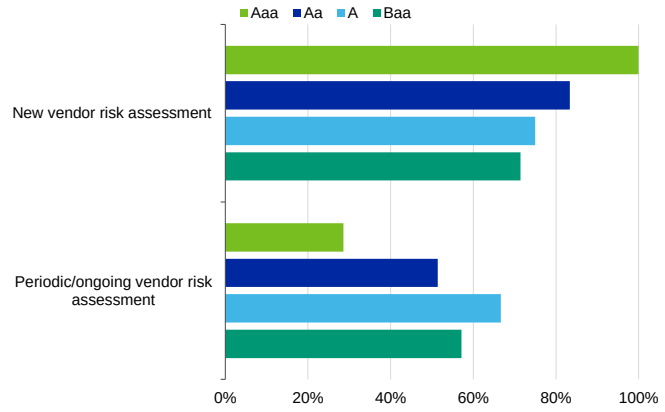
seen mostly in well-resourced industries like banking. However, multifactor authentication (MFA), a more basic cyber defense measure that involves the use of an additional, independent method of authentication to verify a user's identity, is required by the vast majority of higher education institutions, regardless of rating or size, as part of their long-term cyber planning.

Education on safe cyber practices is occurring, especially at the lower end of rating and size categories. Approximately 56% of Baa-rated entities engage with or educate their personnel on cyber issues monthly, compared with just 29% of Aaa, 23% of Aa, and 10% of A-rated entities. It is possible that in instances where an institution does not have the resources to invest in personnel with cybersecurity expertise, they regularly educate existing staff on online threats. Our higher rated institutions tend to engage with staff on an annual basis.

Although survey respondents have, to varying degrees, invested in cybersecurity, they remain vulnerable to attacks on software vendors they partner with. Attacks on third-party vendors have proved disruptive in recent years, and while it is becoming common practice across size and rating categories to require risk assessment of new vendors, existing vendors subject to periodic review less often (see Exhibit 7). Requirements on third-party vendors to report cyber incidents vary, with 83% of Aaa respondents requiring notification compared with 38% of Baa respondents. Requiring vendors to carry cyber insurance can help mitigate risk, but is not a common requirement across the sector (see Exhibit 8).

Exhibit 7

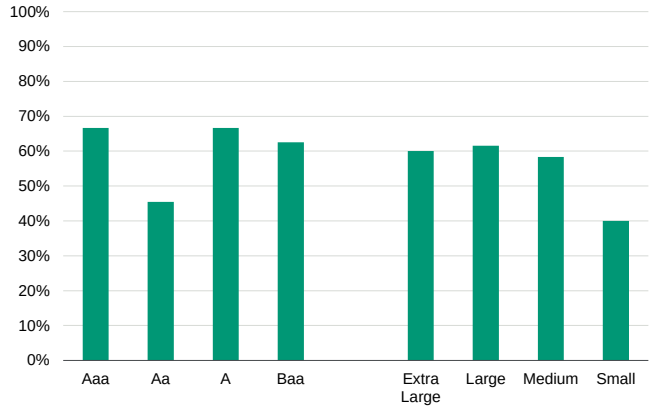
Risk assessments of new third-party vendors are commonly required, but existing vendors are subject to review less often



Source: Moody's Ratings

Exhibit 8

Requiring vendors to carry cyber insurance is not widespread



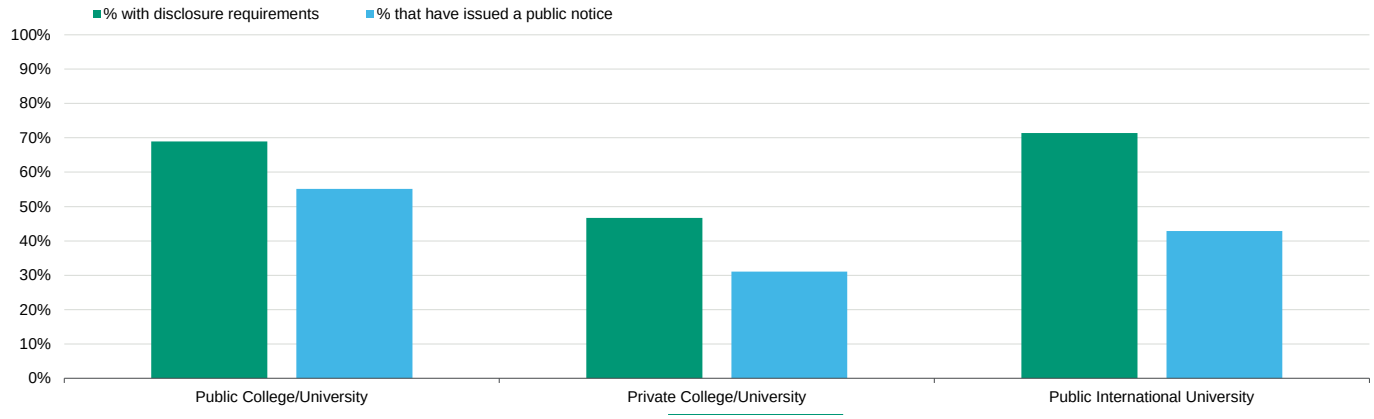
Source: Moody's Ratings

Public universities face stronger requirements on cyber incident disclosure than privates

Incident disclosure rules are generally credit positive because they spur improvements in cyber defense and allow comparisons of how issuers are addressing cybersecurity risks. Publics universities, both US and globally, are more likely than privates to have cyber incident reporting requirements, largely because of their ties to state, provincial or local governments (see Exhibit 9). In light of the rising frequency of attacks, regulatory bodies and higher levels of government have required public disclosure for regional and local governments (RLGs) around the world. Some 60% of all RLGs have reporting requirements for cyber incidents, which in many cases will apply to the universities and colleges in their jurisdictions.

Exhibit 9

Public universities face stronger requirements on cyber incident reporting than privates



Source: Moody's Ratings

Public universities are also more likely than private institutions to have reported incidents to their boards and stakeholders over the past two years. Larger and higher-rated issuers are also more likely to disclose a cyber incident.

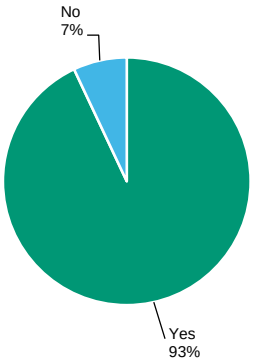
Most issuers have specialized standalone cyber insurance, with the highest rated more likely to buy additional coverage

Cyber insurance is an important element in mitigating the effects of cyberattacks. Nearly all institutions in our survey purchase cyber coverage, with 93% carrying a standalone policy (see Exhibit 10). However, our smallest issuers do lag their larger peers, with around 86% carrying standalone insurance. Regardless, across the sector, the level of coverage has remained largely unchanged since our last survey despite premiums rising sharply over the past three years.

Asked if an issuer has explicit cyber coverage through a traditional insurance policy, 35% of the sector said yes (see Exhibit 11). Notably, about 50% of private colleges have cyber coverage within their traditional policies, compared with only 27% of publics. Public institutions may be more motivated to hold standalone coverage (as 93% do) because traditional policies do not adequately cover cyber threats.

Exhibit 10

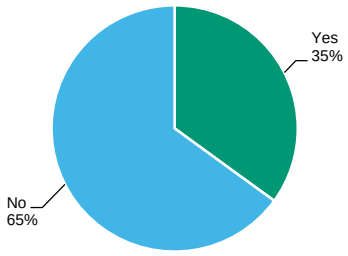
Nearly all respondents carry standalone cyber insurance...



Source: Moody's Ratings

Exhibit 11

...while only 35% of have cyber coverage under traditional insurance policies



Source: Moody's Ratings

The appetite to purchase more coverage is unique to our highest-rated and largest institutions. In the Aa, A, and Baa categories, 84% to 95% of respondents said they would buy the same amount of coverage in 2023 as the prior year. It was only the highest rated and

wealthiest institutions that stated they would purchase more insurance in 2023 (40% of Aaa and 30% of the "extra large"). Unlike their smaller peers, these institutions likely have the financial flexibility to purchase more comprehensive plans. Favorably, none of our respondents, regardless of size or wealth level, indicated that they would buy less coverage.

Larger institutions have more dedicated cyber staff, though institutions generally are having frequent discussions on cyber

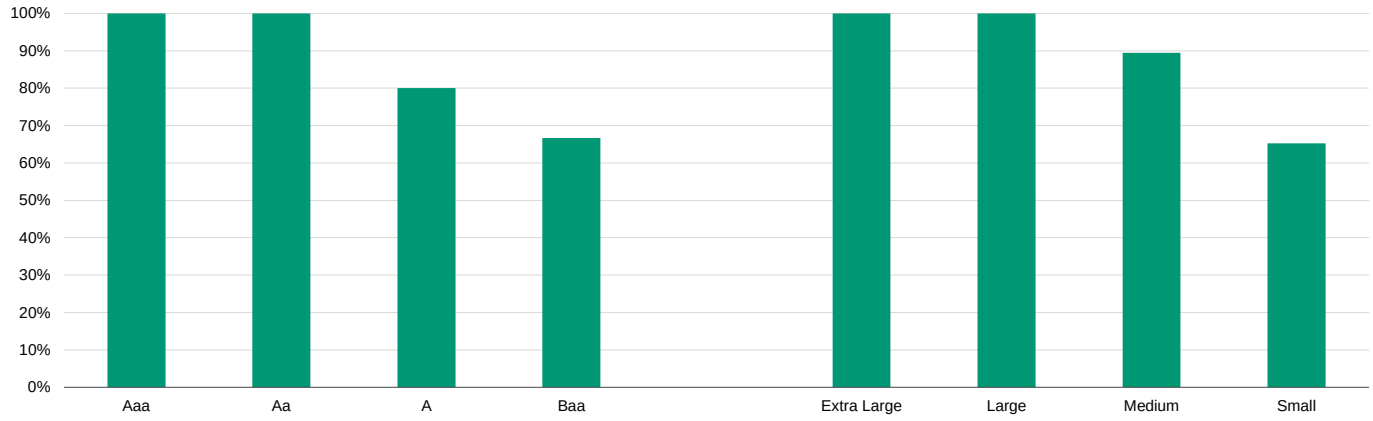
Larger colleges and universities are more likely to have a dedicated cybersecurity manager, who is likely to report to the president on cyber issues. This line of communication fosters greater awareness and understanding of cyber risk within an organization and typically translates into more support for an enterprisewide risk management approach.

Survey results indicate some movement toward hiring staff in-house instead of outsourcing, with an 8% increase in in-house staff across all higher education issuers. Smaller institutions, which are less well resourced with employees likely wearing multiple hats, are less likely to have dedicated cyber employees (see Exhibit 12). Indeed, approximately 35% of small institutions said they do not have dedicated cyber staff. And while there has been a 25% reduction in outsourced cyber staff for small issuers, survey responses indicate no increase in in-house hiring.

Still, cyber managers at smaller institutions are more likely to have monthly conversations about cybersecurity with their presidents, with 64% of small universities and colleges reporting monthly briefings with the president compared with 17% of large and extra large respondents.

Exhibit 12

Less than 70% of Baa-rated issuers and small institutions have dedicated cyber staff



Source: Moody's Ratings

On the whole, there is a lower frequency of reporting among larger and extra large institutions, with cyber managers there more likely to have formal discussions with their boards on a quarterly basis. Since these wealthier institutions have already invested in and built out their cybersecurity teams and policies, frequency of reporting wanes: procedures are in place and operating without disruption. Still, 9% of higher education survey respondents indicate their senior cyber manager never reports to the president. This lags behind other public sector peers, such as not-for-profit hospitals, among which only 1% indicated never reporting to the president.

Non-US universities are well positioned to address cyber risk, with broader disclosure requirements

Many **Australian** universities have adopted a collective approach to managing cyber risk. This includes securing bespoke insurance cover through UniMutual's[1] cyber insurance program and other support and remediation protections. Additionally, through CAUDIT[2] Australian Universities formally retain third parties to manage instances of threats and access skilled personnel to advise on cyber risk management and appropriate responses should a cyber event occur.[3] Finally, there are formal agreements between the country's universities to ensure that full and transparent communication channels are in place between them in the event of a cyber event.

The **Canadian** higher education sector has also seen a rising number of cyberattacks. While most universities have implemented some measure of cyber defenses on a standalone basis (multi-factor authentication, internal awareness campaigns and cyber insurance), we have also seen a broader push for collaboration and to share information to protect against cyber risk. For example, the Canadian Shared Security Operations Center (CanSSOC) offers higher education institutions information sharing, and provides tools and services that support cybersecurity, including advisory services and access to cybersecurity benchmarking, intrusion detection and assessments through various partnerships.

The Canadian Universities Reciprocal Insurance Exchange (CURIE[4]) further supports information sharing across the sector and provides insurance coverage against cyber exposure, data breaches and system interruption. Many universities also work with third-party, private-sector service providers including BitSight (a Moody's affiliate) to monitor their cybersecurity risk exposure, and numerous other industry partners to implement cyber risk mitigation initiatives

Endnotes

1 UniMutual is owned and operated by 26 Australian member universities.

2 CAUDIT is a nonprofit association owned and directed by the CIOs of Australasian universities and research organizations.

3 Of note, Australian legislation is currently being drafted to makes it illegal to pay ransoms.

4 CURIE is a nonprofit reciprocal insurance provider with 78 member institutions across Canada.

REPORT NUMBER 1395744

Contacts

John Manning +61.2.9270.8145
VP-Sr Credit Officer
john.manning@moodys.com

Jonathan Holmes +1 647.417.6302
Ratings Associate
jonathan.holmes@moodys.com

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

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

CLIENT SERVICES

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

MOODY'S
INVESTORS SERVICE