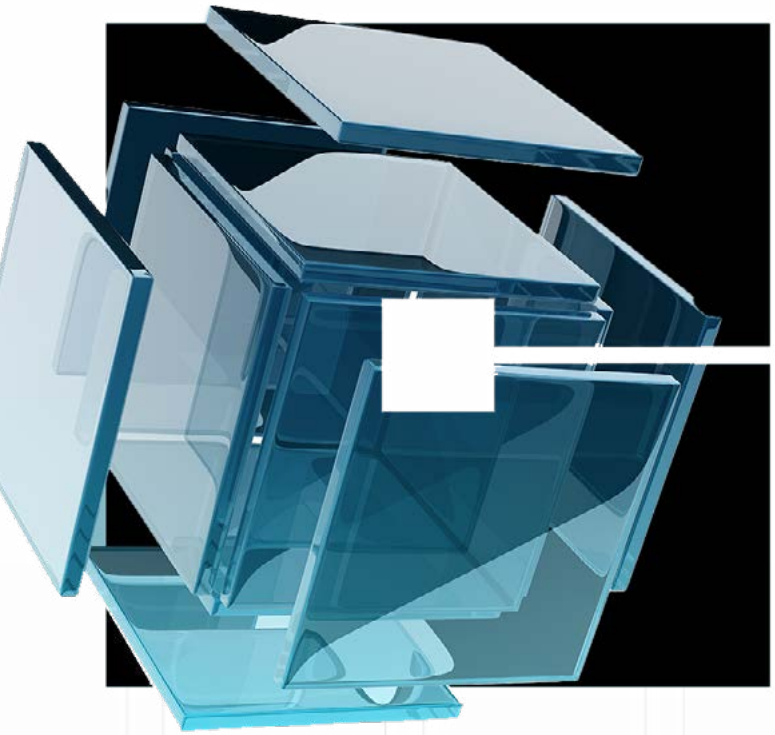
CyberCube

H1 2025

Global Threat Briefing

Understanding cyber risks for small businesses.



SMALL BUSINESSES WITH

$10m to $250m

in annual revenue contribute a significant share of global economic output.

The small business cyber protection gap

In developed markets, small businesses drive economic growth, exports, and employment. In emerging markets, they form the backbone of expanding sectors and play a key role in future prosperity. However, they remain underserved by the global cyber (re)insurance market — facing attacks and their consequences without sufficient insurance coverage.

This protection gap presents both an opportunity and a responsibility for brokers and (re)insurers. Brokers play a crucial role in driving adoption among small businesses, helping them recognize the value of cyber coverage. For (re)insurers, expanding to small enterprises not only broadens market reach and enhances portfolio diversification but also strengthens economic resilience. These businesses can benefit most from the pre-incident services offered by insurance institutions, the vulnerability scanning provided during the underwriting process from companies including CyberCube, and the post-incident recovery services. When small businesses effectively prevent and recover from attacks, they protect jobs, sustain supply chains, and support their communities.

This report examines cyber security trends impacting small businesses and their cyber (re)insurers. Our biannual *Global Threat Briefing* is part of CyberCube's Concierge threat intelligence service, which was built for the global cyber (re)insurance industry.

KEY INSIGHTS ↘

Key insights:

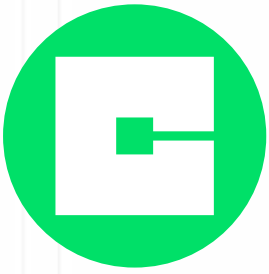
Financially-motivated ransomware gangs represent a problem for small businesses.

Small Financials represent an opportunity for cyber brokers and (re)insurers. However, due to their reliance on common technology, even secure small Financials are at risk of losses from cyber aggregation events.

Small Education is among the highest-risk sectors that require greater scrutiny.

Education industry outage and data breach risk stems from Student Information & Learning Management Systems (e.g., PowerSchool).

In 2025, cyber (re)insurers should continue to monitor how Artificial Intelligence (AI) could enable threat actors to scale attacks against small businesses in the coming year(s).



This report highlights our commitment to advancing cyber risk quantification and addressing the protection gap for small businesses. Together, we can transform market potential into meaningful impact — building a safer, more secure, and more resilient global digital economy.

Cyber threats to small businesses: threat overview

Cyber attacks on small businesses occur worldwide across industries. **Exhibit 1** shows how threat actors have attacked small business sectors, including Financials, Banking, Education, Transportation, IT, Healthcare, Public, and Non-Profit. For example, between 2024 and February 2025, small businesses were attacked, with impacts ranging from sensitive data breaches to large-scale financial system outages.

EXHIBIT 1

Select cyber attacks on small businesses by country: 2024 through February 2025

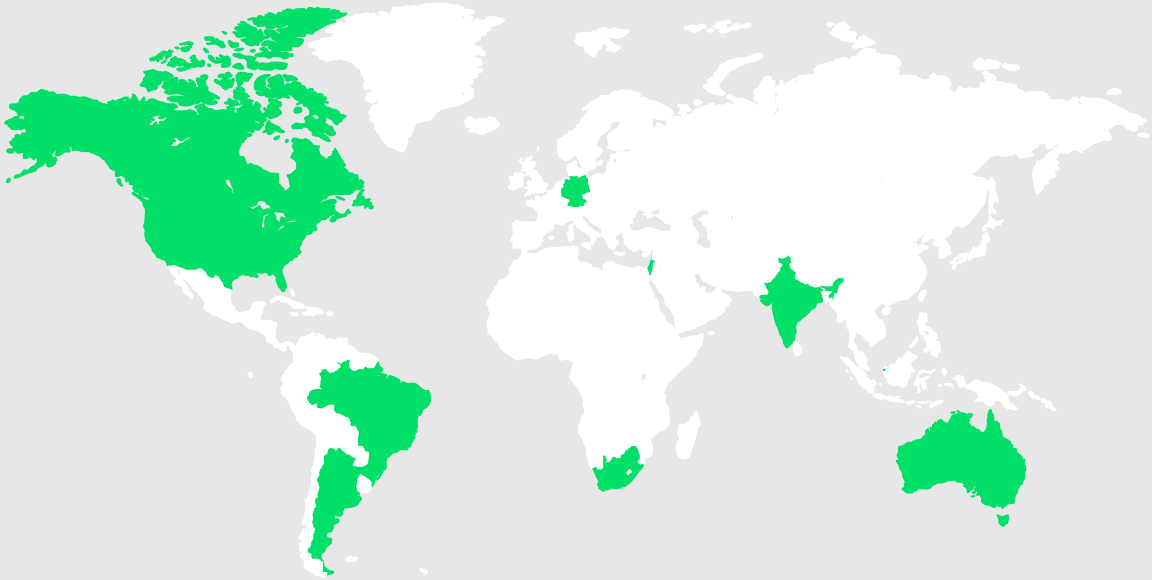
United States
FINANCIALS
Accident Fund's online systems were shutdown.

United States
NON-PROFIT
Angel Horses Inc., a Billings-based non-profit dedicated to aiding the elderly loses $70K.

Switzerland
INFORMATION TECHNOLOGY (IT)
Xplain, an IT provider to the government was breached.

Germany
TRANSPORTATION & LOGISTICS
DDoS downed websites of three regional railway companies.

Israel
FINANCIALS
Shva (Automatic Bank Services Ltd.), attacked and payment processing systems downed.



India
BANKING
300 small banks were forced to go offline due to a ransomware attack on C-Edge Technologies.

Australia
EDUCATION
The Australian Association of Independent Schools in New South Wales targeted in attacks.

Singapore
FINANCIALS
The cryptocurrency platform Phemex was forced to pause operations and lost $69M.

United States
HEALTHCARE
Memorial Hospital and Manor notified 120,000 individuals that their personal data was stolen.

Canada
EDUCATION
Hamilton-Wentworth District School Board taken offline.

Brazil
PUBLIC SECTOR
Ransomware on a small city government in Brazil.

Argentina
PUBLIC SECTOR
Municipality attacked and results in losing 19M pesos.

South Africa
PUBLIC SECTOR
Weather Service attack hits aviation/marine services.

Data from **Coveware** shows companies with 11 to 1,000 employees account for 75% of ransomware victims in their response cases, highlighting that small and mid-sized businesses (SMBs) are targets for cybercriminals. Small companies lack advanced cybersecurity defenses, making them vulnerable to breaches at scale — allowing attackers to compromise companies simultaneously.

Threat actors are beginning to leverage AI to automate key parts of attacks, and could demand smaller ransoms that, while individually modest, add up significantly when executed in volume. Our focus on small companies is not meant to downplay the impact of ransomware on large enterprises but to emphasize how it poses an existential threat to smaller businesses with limited resources.

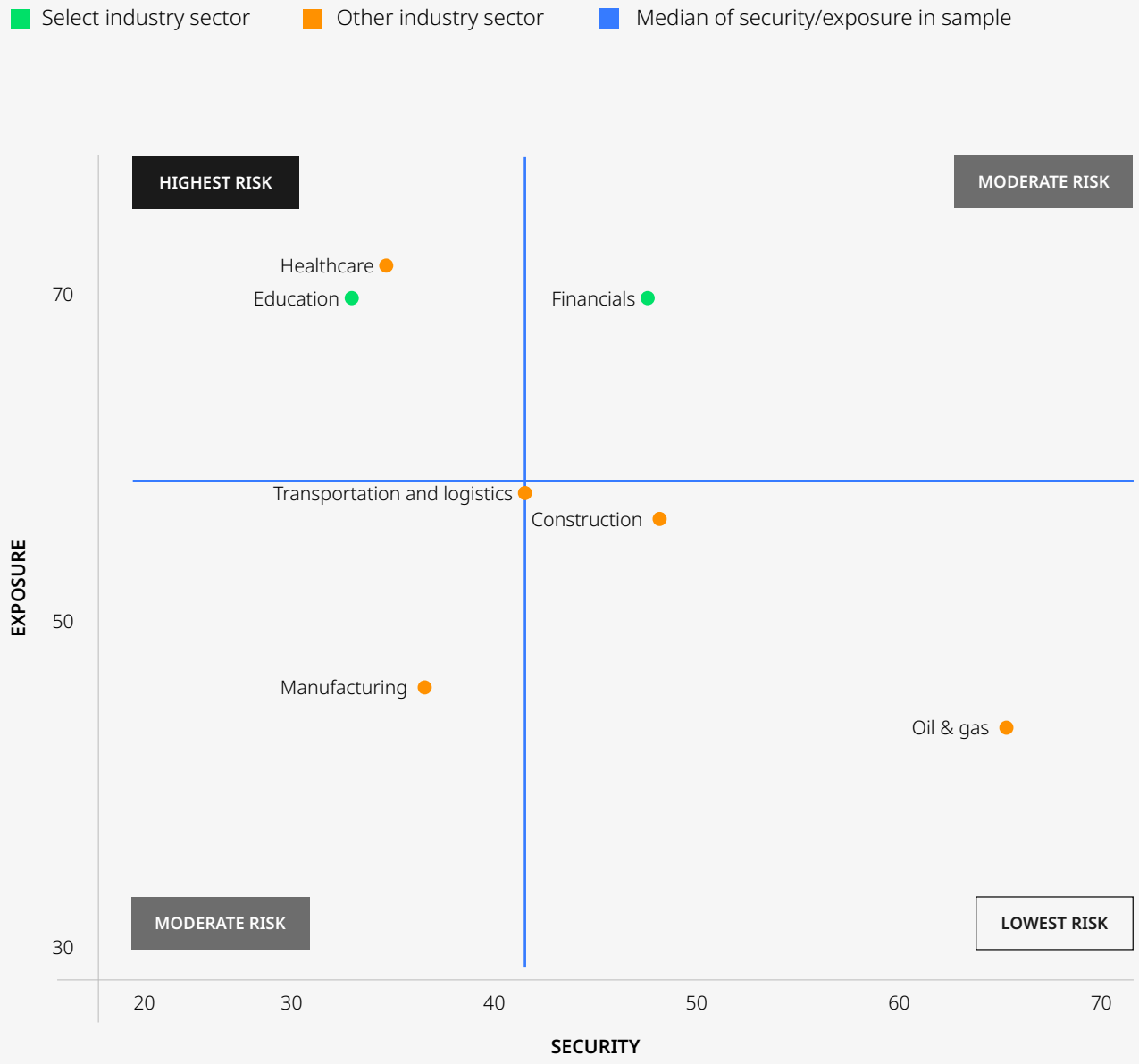
Financials represent an opportunity zone for cyber brokers and (re)insurers, whereas Education is among the highest-risk sectors requiring scrutiny

The combination of Exposure and Security provides a clear view of industry-level cyber risk differentiation, identifying both opportunities and sectors requiring greater scrutiny.

Analyzing a portfolio of 143,000 small Financials firms globally, **Exhibit 2** shows the Financials sector sits in the "Moderate Risk" quadrant, indicating moderate security measures partially offsetting high exposure. This sector presents an opportunity, as insurers can effectively differentiate between strong and weak performers and price cyber policies accordingly. Meanwhile, Education (and Healthcare) fall into the "Highest Risk" category, requiring heightened scrutiny and due diligence in underwriting.

EXHIBIT 2

Median security and exposure score matrix: select small business sectors, January 2025



Exposure score: inherent cyber risk. Higher = higher risk, all else equal.

Security score: ability to secure digital assets. Higher = less risk, all else equal.

Source(s): CyberCube Global Insurance Exposure Database (IED) Portfolio, Standalone only
Small companies (annual revenue of $10M - $250M), n= 143,301
CyberCube Account Manager v5.5 Security & Exposure Scores, January 2025

Opportunity industry deep dive: small Financials

In 2024, cyberattacks struck small Financial firms worldwide and caused severe disruptions to operations, and sensitive data exposure.

↗ Iran

A cyberattack in August on the fintech software company Tosan brought severe disruptions and loss of data to 20 of Iran's 29 credit institutions, underscoring the susceptibility of financial systems to supply chain attacks on small Financial firms.

↗ India

An attack on the payments provider C-Edge Technologies downed the banking operations of 300 cooperative and regional banks, illustrating the broad reach of cyber attacks on small firms that are also critical digital financial infrastructure.

↗ United States

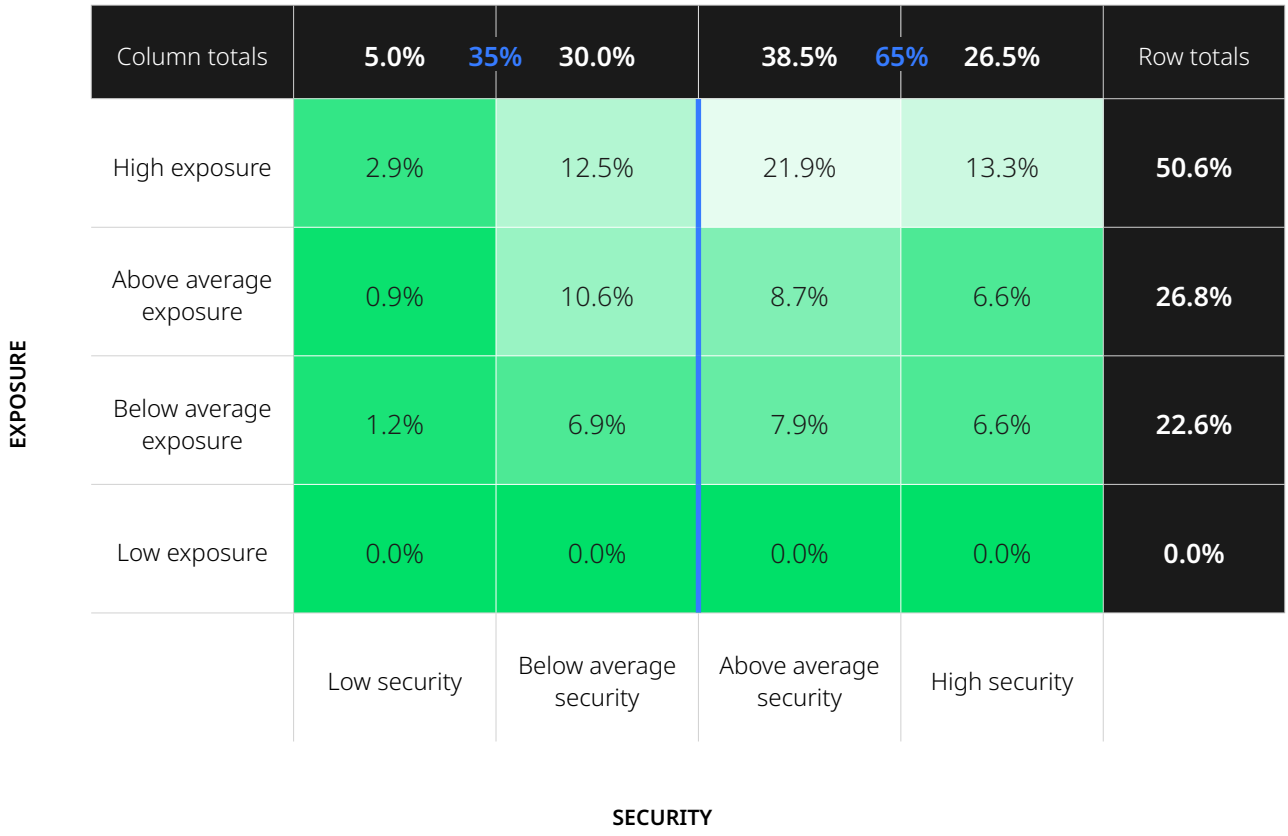
LockBit ransomware hit securities lending firm EquiLend in January and fintech bank Evolve Bank & Trust in May, with both attacks affecting a broader ecosystem of small-sized fintech customers and partners.

GLOBALLY

Small Financials are highly exposed and have a wide range of security. For example, in **Exhibit 3** we observe 65% of small Financials firms are concentrated in above-average or high-security quadrants, 35% fall into below-average or low-security.

EXHIBIT 3

Percentage of global small Financials within combinations of security and exposure score categories, January 2025



Source(s): CyberCube Global Insurance Exposure Database (IED) Portfolio, Standalone only
Financials, Small companies (annual revenue of $10M - $250M), n= 9,993
CyberCube Account Manager v5.5 Security & Exposure Scores, January 2025

For cyber underwriters, this variability in security maturity across small Financials requires close attention, as even entities with higher defenses remain vulnerable in such a critical sector. The disparity across security levels makes a tailored approach to underwriting essential for identifying high-security small Financials.

High-security financial institutions adhere to industry regulations such as PCI DSS (for payment security), SOC 2 (for data handling), and ISO 27001 (for information security management). They conduct regular compliance audits, implement strong fraud detection mechanisms, and follow strict reporting protocols. Low-security institutions may lack formal compliance programs, have outdated security policies, or fail to meet regulatory requirements, making them more vulnerable to regulatory penalties and cyber threats.

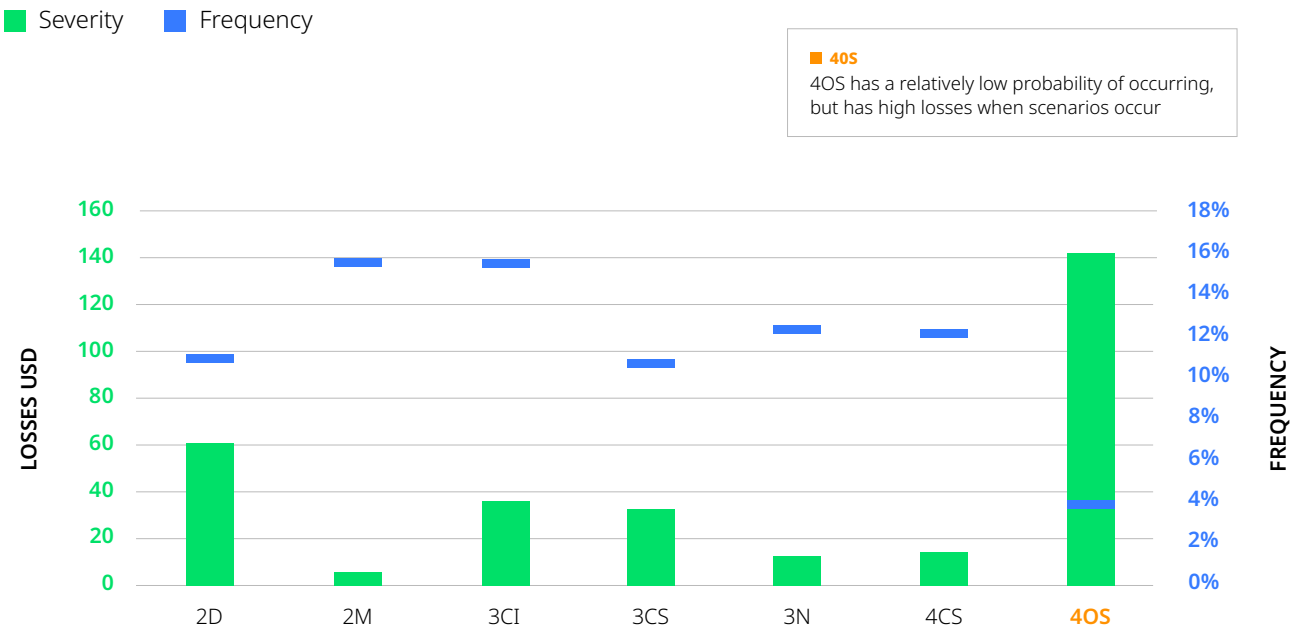
Even the most secure small Financial firms are at risk of cyber aggregation events due to sector-wide reliance on common technology

CyberCube's **Portfolio Manager** (PM) allows cyber (re)insurers to assess the financial impact of catastrophic cyber aggregation events tied to the compromise or outage of widely used technologies. PM maps technologies within a company's network to scenarios where those technologies are attacked.

An analysis of a portfolio of over 9,000 small Financial firms globally shows that common technology dependencies put these organizations at risk for significant cyber aggregation events (see **Exhibit 4**).

EXHIBIT 4

Average conditional severity and frequency of PM event families for small Financials, global IED



Modeling notes

- The x-axis represents frequency (likelihood of occurrence), the y-axis represents severity (financial impact).
- Portfolio Manager (PM v5.5), default settings, 50k simulations, Economic losses
- Portfolio: Global Insurance Exposure Database (IED), Small Financials ($10M - $250M), Standalone only
- n = 9,993

CyberCube PM event family IDs and descriptions

Family ID	Description
2D	Breach | Data aggregator
2M	Breach | Money systems
3CI	Outage | Cloud infrastructure
3CS	Outage | Cloud software
3N	Outage | Network services
4CS	Ransomware | Cloud software
4OS	Ransomware | Operating systems and programmable languages

A large portion of the portfolio relies on fund administration platforms such as SS&C GlobeOp, or HedgeServ, making them vulnerable to CyberCube's PM Scenario 10 in family 2D, which models large-scale data theft against a leading asset manager fund administrator.

Highest risk industry deep dive: small Education

Small Education organizations frequently come under attack from cybercriminals due largely to constrained cybersecurity budgets and the valuable student and employee information they possess. From 2024 through early 2025, attacks involved cybercriminals targeting schools worldwide, exposing sensitive data and creating widespread operational disruptions that negatively impact the well-being of students and educators.

Exhibit 5 shows that small education organizations are concentrated in below-average or low-security quadrants (56%). This suggests that many organizations in this sector are underinvesting in cybersecurity relative to their risk profiles. However, a smaller portion — 44% — fall into above-average or high-security quadrants.

EXHIBIT 5

Percentage of global small Education within combinations of security and exposure score categories, January 2025

Column totals	46.2%	56%	9.6%	18.8%	44%	25.4%	Row totals
High exposure	34.2%		1.8%	8.1%		6.3%	**50.4%**
Above average exposure	10.4%		1.8%	3.0%		5.7%	**20.9%**
Below average exposure	1.5%		6.0%	7.6%		8.8%	**23.8%**
Low exposure	0.0%		0.0%	0.2%		4.7%	**4.9%**
	Low security		Below average security	Above average security		High security	

EXPOSURE

SECURITY

Source(s): CyberCube Global Insurance Exposure Database (IED) Portfolio, Standalone only
Education, Small companies (annual revenue of $10M - $250M), n= 5,008
CyberCube Account Manager v5.5 Security & Exposure Scores, January 2025

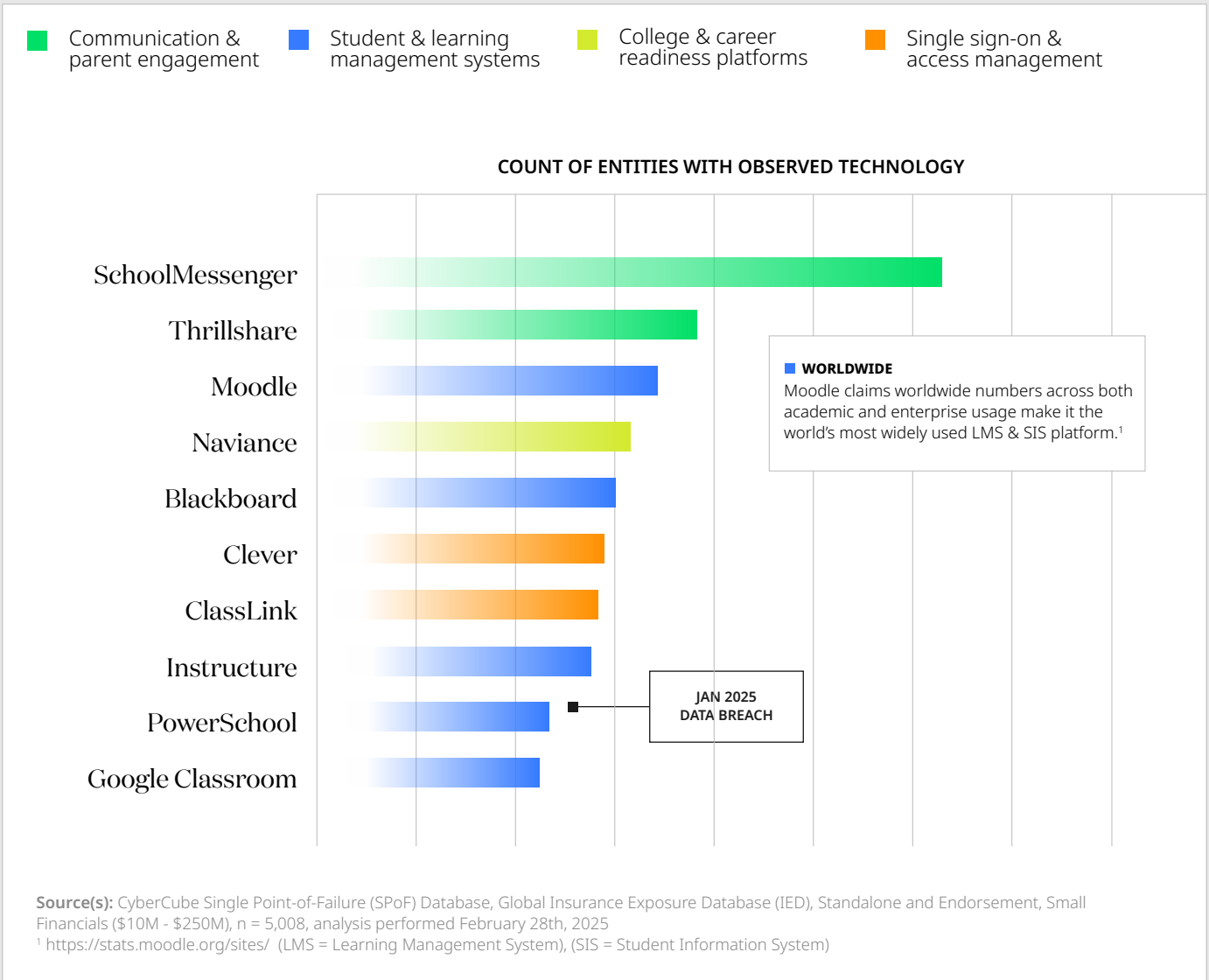
For cyber underwriters, small Education should be regarded as high-risk overall, given the sector's concentration in lower-security maturity categories.

Industry-specific technology risk poses a concern for small Education

The ten technologies highlighted in **Exhibit 6** are essential and widely used by small education organizations globally. Half of the top ten technologies are Student Information & Learning Management Systems (LMS & SIS). LMS & SIS represent outsize data breach and outage risks for small Education. These systems handle coursework, grading, sensitive records, and learning resources.

EXHIBIT 6

Most utilized education technologies among global small Education by count of dependent entities



Source(s): CyberCube Single Point-of-Failure (SPoF) Database, Global Insurance Exposure Database (IED), Standalone and Endorsement, Small Financials ($10M - $250M), n = 5,008, analysis performed February 28th, 2025

[1] https://stats.moodle.org/sites/ (LMS = Learning Management System), (SIS = Student Information System)

Affecting over 60 million students globally

In January 2025, PowerSchool, a cloud-based student information system (SIS) used by 18,000 schools, suffered a data breach. Attackers stole sensitive student records from the platform, affecting over 60 million students globally. Schools using PowerSchool may face regulatory scrutiny under FERPA (U.S.), GDPR (Europe), and other student protection laws. Insurers covering schools may face losses from lawsuits related to minors' data exposure. More schools may seek broader data breach coverage, forcing cyber (re)insurers to adjust risk models and tighten cyber underwriting standards.

High-security small Education organizations conduct regular vendor risk assessments, enforce contractual security obligations, and monitor third-party security practices. Low-security organizations, however, may use outdated software, fail to vet vendors, or lack visibility into the security measures of external service providers, increasing exposure.

Cyber threat outlook for small business H1 2025

In 2025, AI is not expected to revolutionize cyber attacks against small businesses. However, we are closely monitoring how threat actors could leverage AI to evolve the efficiency and scalability of their attacks - particularly in automating target reconnaissance, accelerating authentication bypass, deploying exploits, and executing ransomware.

AI could theoretically accelerate the growth of threat actors targeting small businesses with lower- and mid-value ransoms by making attacks cheaper, more efficient, and more scalable. In 2025, (re)insurers should be aware of signs of AI enabling threat actors to scan for vulnerable systems at internet scale faster than traditional methods, increasing the exposure of small and mid-sized businesses to opportunistic attacks.

Next steps to close the small business cyber protection gap

Closing the cyber protection gap for small businesses requires a concerted effort from key industry stakeholders, including cyber brokers, underwriters, and reinsurers. Each plays a critical role in expanding access, improving risk selection, and ensuring market stability.

Brokers must focus on expanding education and access to cyber insurance by incentivizing generalist brokers to dedicate more time to selling cyber policies, improving client communication on cyber risks, and offering pre-coverage risk assessments to ensure appropriate coverage.

Underwriters can enhance risk selection and pricing by developing scalable underwriting practices and models tailored to small businesses. Encouraging these firms to adopt strong cybersecurity measures and collaborating with brokers to refine policy language and services will be instrumental in making cyber coverage more effective and accessible.

Reinsurers have a vital role in maintaining market stability and capacity. Establishing a clear stance on effective cyber underwriting strategies for small-business-focused portfolios will help differentiate them from large enterprise approaches, ensuring that cyber risk is managed appropriately across different segments.

By taking these steps

The industry can build a more resilient cyber insurance market that better protects small businesses against evolving threats. Addressing these gaps proactively will not only enhance coverage options but also contribute to broader cybersecurity resilience across the small business sector.

Author: William Altman, Director of Cyber Threat Intelligence Services

Editorial Content: Yvette Essen, Head of Communications and Market Engagement

Data & Analytics: Yonbo Yang, Actuarial Consultant