
CyberCube
Global Threat Briefing
H2 2025
Applying Analytics and Threat Intelligence to Grow in a Soft Market
50%
85%
15%
75%

Authors

CyberCube

Author:

William Altman
Head of Cyber Threat Intelligence Services

Data & Analytics:

Yonbo Yang
Actuarial Consultant

Ben Strickson
Cyber Risk & Analytics Engineer

Editorial Content:

Yvette Essen
Head of Communications
& Market Engagement
at CyberCube

Editorial Design:

Felix Paula
Growth Marketing Creative
at CyberCube

Introduction

Dear Readers,

Over the long term, cyber insurance represents one of the most attractive opportunities in the property and casualty sector. Cyber risk continues to rank among the top concerns for corporate leaders and insurance buyers, and its importance is only increasing. This is a secular, generational trend driven by our growing dependence on technology, data, and artificial intelligence. The more digital the world becomes; the more essential cyber resilience and cyber insurance will be.

In the near term, the current soft market shapes the reality in which our clients operate. (Re)insurers are tightening focus, prioritizing efficiency and margin stability over pure premium expansion. This environment raises an important question: how can CyberCube's unique mix of advanced analytics and threat intelligence provide the precision needed to navigate leaner conditions while helping brokers and (re)insurers maintain profitability, underwriting discipline, and the ability to uncover new opportunities? That is precisely the question we seek to answer in this Global Threat Briefing.

Looking ahead, part of the market's growth will come from higher limits as cyber exposures expand. To ensure that growth is sustainable, the industry must also diversify by reaching underinsured segments such as small and medium-sized enterprises (see our H1 2025 Global Threat Briefing), expanding into new geographic regions, developing coverages for emerging risks, and serving industries traditionally viewed as challenging but which can be written profitably with the right analytics and threat intelligence.

At CyberCube, our mission remains steadfast: to partner with the global cyber (re)insurance industry in building a sustainable and resilient market, grounded in analytics, innovation, and a deep understanding of cyber risk.

— Pascal Millaire, CEO, CyberCube

Executive Summary

After three consecutive years of rate reductions, the cyber market remains soft, with capacity outpacing demand. Heightened competition has driven concessions on premiums, limits, and coverage terms. Meanwhile, cyber threats and particularly ransomware continue to expand in both scale and geography.

CyberCube's Analysis Shows:

Ransomware is growing beyond traditional hotspots and in emerging economies including Latin America, Africa, the Middle East, and Asia.

Sustainable growth requires diversification and innovation across industries, regions, SMEs, and emerging risks.

The Public Sector illustrates both the challenges and opportunities shaping today's cyber insurance market. It combines high exposure and uneven security maturity with increasing reliance on digital systems.

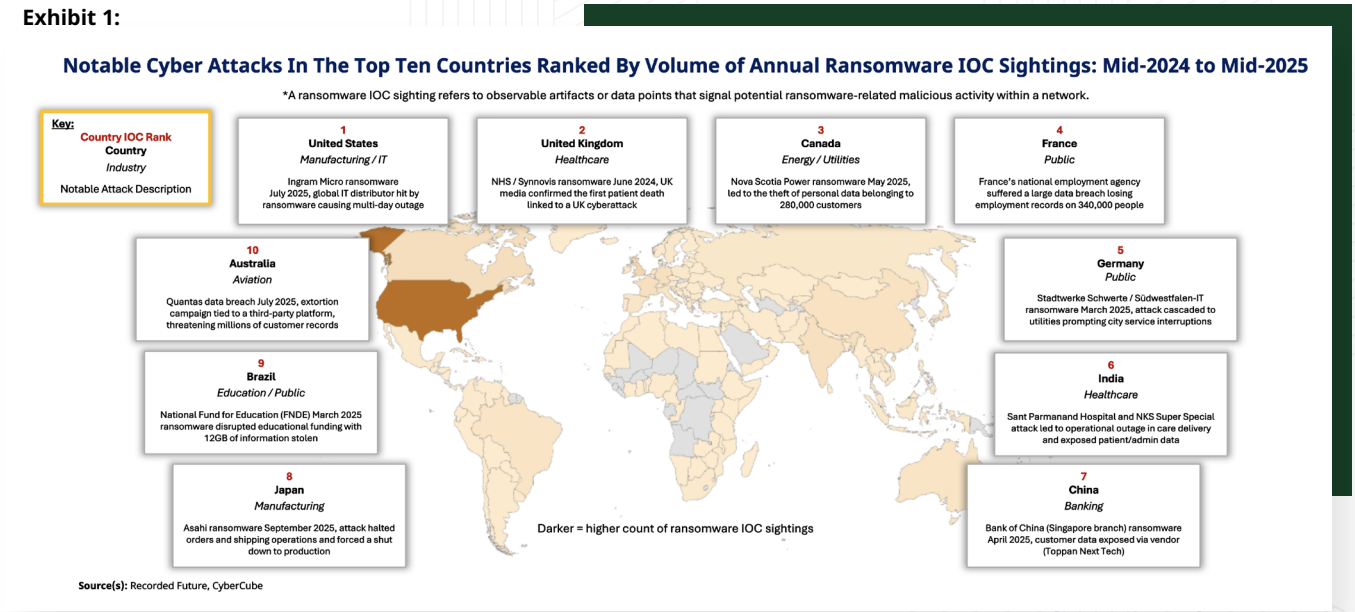
Amid budget cuts and personnel shortages, network misconfigurations remain a leading vulnerability for Public Sector organizations. Yet despite the sector being highly Exposed and under Secured relative to the global average, there are pockets of opportunity.

Market Overview: A Soft Market Meets Rising Threats

Rising competition has pushed cyber into its third consecutive year of rate reductions, as insurance supply continues to outpace demand. This dynamic is offsetting recent exposure growth through negative rate changes and driving further concessions on premium, limits, coverage, and security controls.

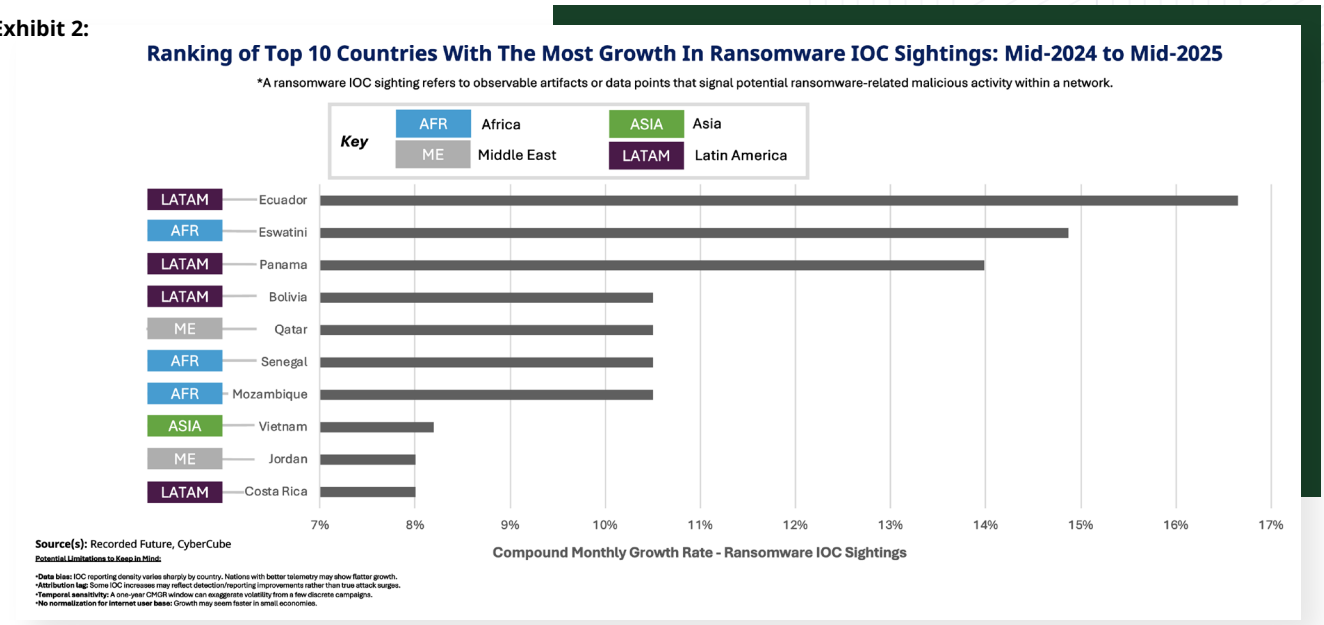
At the same time, as **Exhibit 1** shows, ransomware is a global cyber threat, with incidents now spanning virtually every region and sector. CyberCube's analysis shows the United States still records the highest volume of ransomware indicators of compromise (IOCs), reflecting its economic scale and digital maturity.

Exhibit 1:



Furthermore, ransomware is expanding beyond traditional hotspots into emerging economies. **Exhibit 2** highlights where ransomware is spreading the fastest, based on compound monthly growth rates of ransomware IOCs from mid-2024 to mid-2025.

Exhibit 2:



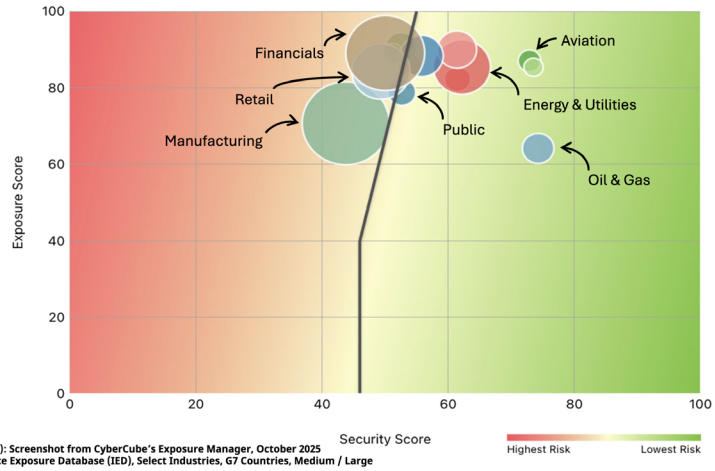
Concentrated in emerging economies across Latin America, Africa, the Middle East, and Asia, these trends underscore ransomware's shift beyond traditional hotspots and toward regions undergoing rapid digitalization, uneven defense, and growing strategic importance.

CyberCube has identified four macro forces associated with the acceleration and regional concentration of ransomware activity. Growth in ransomware is fueled by a combination of weak rule-of-law and governance structures, corruption and financial-system opacity, geopolitical stress and conflict dynamics, and rising digital and economic interdependence that broadens systemic exposure.

Exhibit 3 demonstrates some industries (positioned right of the line) are above average security posture, notably Energy & Utilities, Oil & Gas, and Aviation. Industries deemed below average (left of the line) include Financials, Retail, Manufacturing. Those situated "on-the-line" include Services, Arts & Entertainment, and the Public Sector.

Exhibit 3:

CyberCube Exposure Manager: Average Exposure / Security Score of Select Industries: G7 Countries, Medium / Large Size



- Some industries are above average security posture (right of line): e.g., Energy & Utilities, Oil & Gas, Aviation
- Industries below average (left of line) include Financials, Retail, Manofacturing
- Industries "on-the-line" include Services, Arts & Entertainment, and the Public sector

All industries are displayed: Manufacturing, Financials, Retail, Energy & Utilities, Services, Banking, Healthcare, Oil & Gas, Public, Transportation & Logistics, Aviation, Arts & Entertainment, Education, Non-Profit

Source(s): Screenshot from CyberCube's Exposure Manager, October 2025 Insurance Exposure Database (IED), Select Industries, G7 Countries, Medium / Large n=12,000

Analysis: The Public Sector

This report focuses on the Public Sector as a case study. The sector illustrates both the challenges and opportunities shaping today's cyber insurance market. It combines high exposure and uneven security maturity with increasing reliance on digital systems.

CyberCube's analysis shows a number of key takeaways:

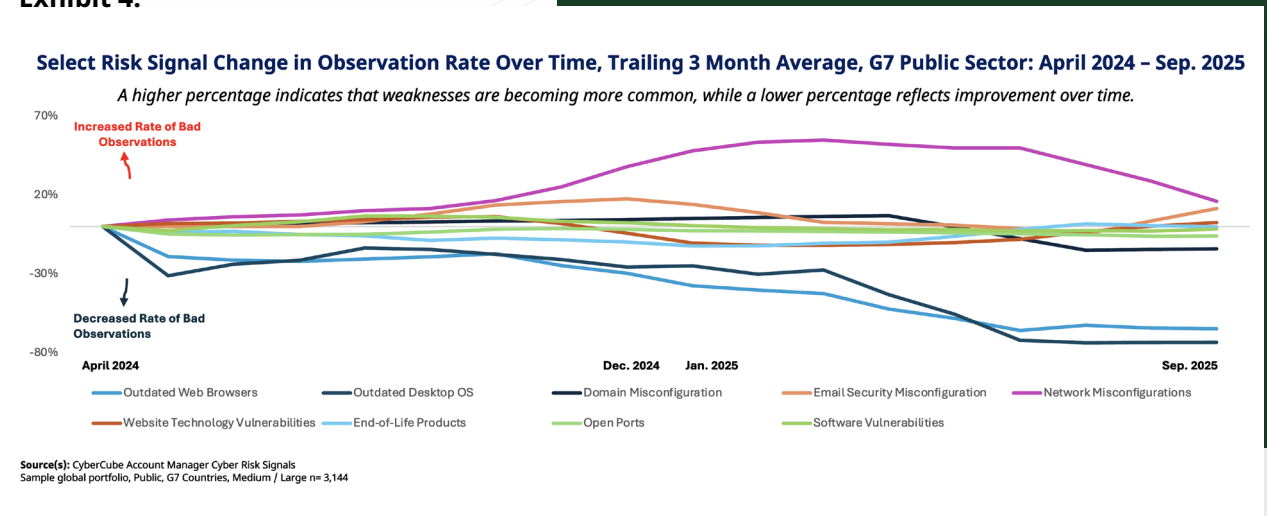
- Public entities face significant cyber exposure risk, yet some remain inadequately secured.
- The Public Sector's high systemic exposure creates meaningful growth opportunities.
- Diving into diverse sub-sectors could enable targeted underwriting vs. treating every sub-sector as "all bad".

Global Public Sector Spotlight

Since 2023, there have been more than 1,300 publicly reported cyberattacks on public-sector organizations. The United States and Germany report the highest volumes due to their large government networks and strong disclosure requirements. Other nations such as France, the United Kingdom, Canada, Italy, and Japan also face growing risks, including espionage campaigns against critical infrastructure.[1]

Exhibit 4 tracks changes in the rate of negative cyber risk observations across key signals for the global Public Sector. These signals — spanning outdated technologies and configuration failures — are critical to monitor as Public Sector organizations face budget cuts and personnel shortages. Controls that require regular maintenance such as patching of Software Vulnerabilities often degrade first, magnifying certain types of operational and insurable risk.

Exhibit 4:



Although the frequency of attacks continues to rise, some indicators of cyber hygiene are improving. Public institutions are updating outdated systems more consistently, while network misconfigurations remain a leading vulnerability.

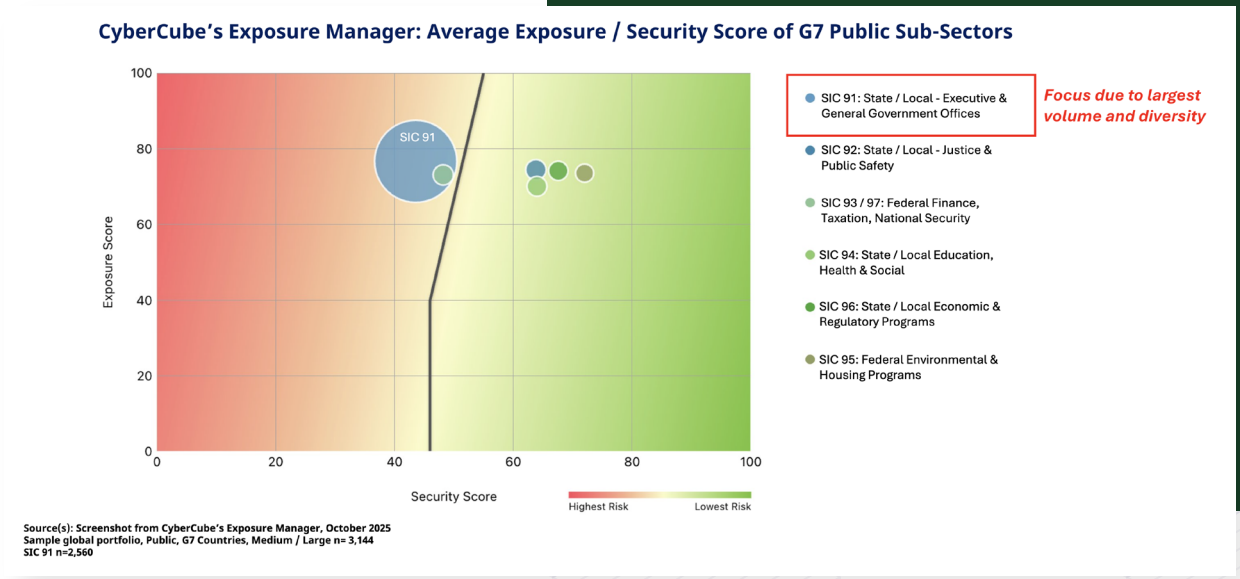
The Public Sector represents a diverse market spanning every level of government and a range of administrative, regulatory, and social functions. Despite the Public Sector being highly Exposed and under Secured relative to the global average, there are pockets of opportunity.

[1] https://konbriefing.com/en-topics/cyber-attacks-public-administration.html

Subsector Focus: State and Local Governments (SIC 91)

State and local government executive and general offices (SIC 91) present strong potential for underwriting innovation within the Public Sector (see **Exhibit 5**). Realizing this potential requires strict risk controls and disciplined pricing.

Exhibit 5:

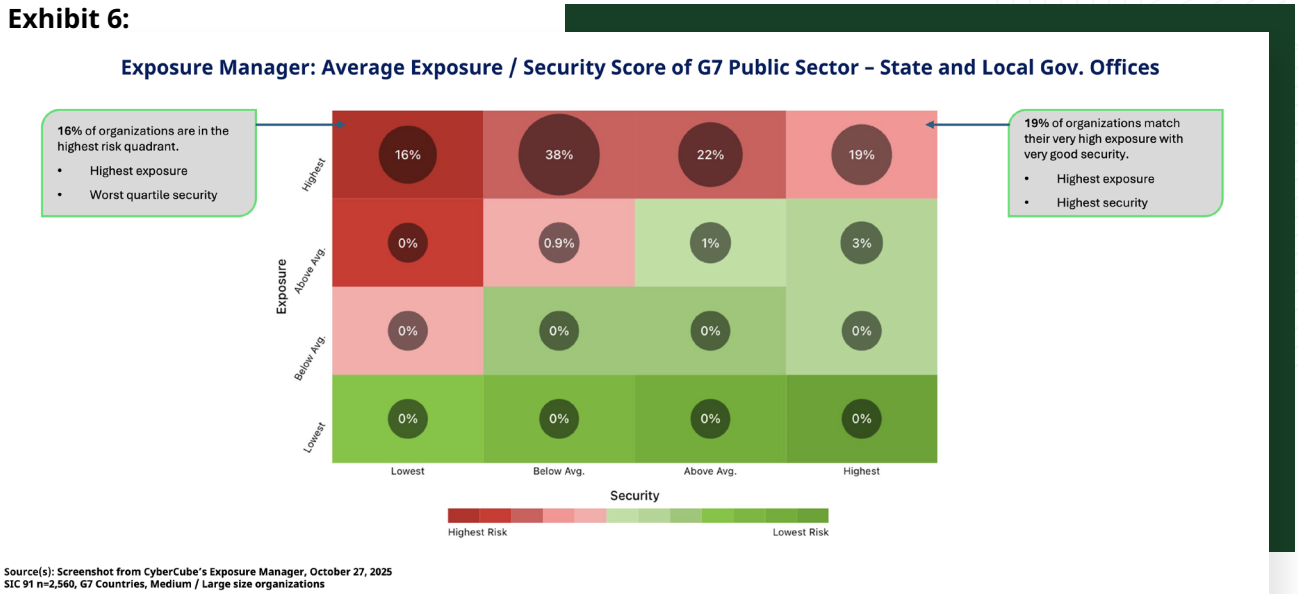


(Re)insurers can differentiate through granular underwriting strategies, tiered pricing, and risk-based segmentation, while focusing on lower-risk administrative programs and appropriately pricing riskier clusters.

State and local government's (SIC 91) exhibit wide variation in Security posture

Exhibit 6 illustrates the variation in security posture among state and local government organizations across the G7, as measured in CyberCube's Exposure Manager.

Exhibit 6:



Approximately 16% of organizations in this segment combine high exposure with weak security, while 19% maintain high exposure but strong cyber controls. This variation enables (re)insurers to differentiate through segmentation and targeted underwriting strategies.

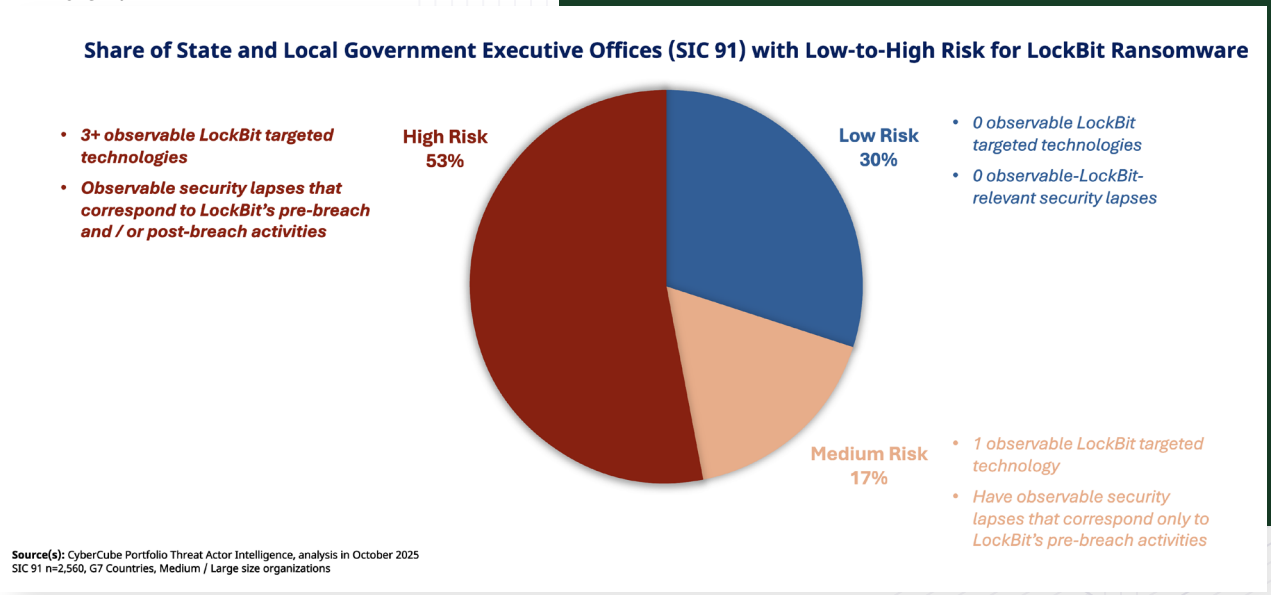
Portfolio Threat Actor Intelligence: Refining Exposure Management

LockBit 5.0 remains one of the most significant ransomware threats to Public Sector organizations, particularly those using legacy systems or operating with limited cybersecurity resources.

CyberCube's Portfolio Threat Actor Intelligence (PTI) solution helps (re)insurers determine which organizations in their portfolios are most likely to be targeted by specific threat actors. PTI segments portfolios into low-to-high risk tiers based on factors such as technologies used, industry, organization size, and known vulnerabilities.

53% of state and local government offices (SIC 91) worldwide face high risk from LockBit ransomware due to both targeted technology use and security lapses.

Exhibit 7:



Using a proprietary scoring framework, CyberCube evaluates susceptibility to LockBit's tactics, techniques, and procedures (TTPs) by identifying organizations that both rely on technologies frequently exploited by LockBit and exhibit weaknesses across its pre- and post-breach kill chain. This dual exposure increases the likelihood that LockBit affiliates could successfully execute and complete a full-scale intrusion.

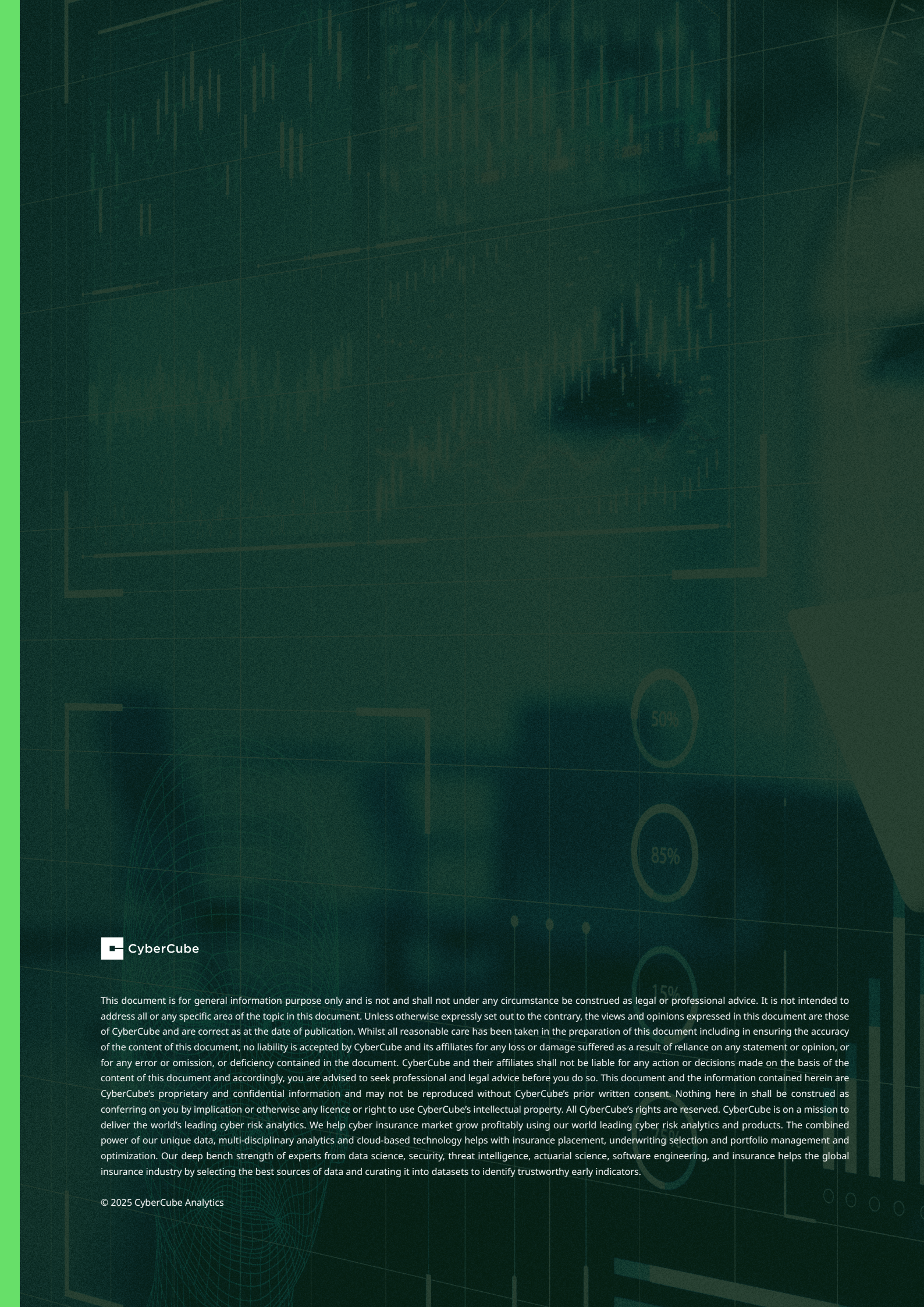
Conclusion: Growing with Precision

As the market approaches 2026, success in cyber (re)insurance will depend on precision, insight, and the ability to align opportunity with exposure.

Cyber insurance is poised to remain one of the most dynamic and strategically vital segments within the property and casualty sector. As businesses deepen their reliance on digital infrastructure, data, and artificial intelligence, the frequency and complexity of cyber risks will continue to escalate. This evolution underscores the enduring demand for sophisticated risk quantification and mitigation solutions that translate cyber exposure into financial terms. The shift toward a more digital economy ensures that cyber resilience and the insurance products that enable it will become integral components of corporate risk management strategies worldwide.

At the same time, the current soft market environment demands precision, discipline, and innovation. CyberCube's analytics and threat intelligence capabilities, including Exposure Manager, *Portfolio Threat Actor Intelligence*, and the *Global Insurance Exposure Database*, are designed to empower (re)insurers and brokers to thrive even amid soft market conditions, identifying profitable growth opportunities while maintaining underwriting integrity. As the sector matures, future expansion will hinge on serving underinsured segments, new geographies, and emerging risk classes.

The path forward companies which belong to those who combine rigorous data-driven insight with creative market strategies, transforming complexity into clarity, and uncertainty into sustainable growth.



CyberCube