CyberCube

The Cyber Data Paradox

Balancing forward-looking signals with stable underwriting insight

CyberCube

Contents

Executive summary

Cyber insurers have more data available today than ever before. External telemetry, security signals, firmographic data, and threat intelligence are now widely accessible across the market. However, underwriting decisions have not necessarily become easier with this data.

The challenge is not access to data — it is determining which data actually matters, how it should be used, and where it fits within the underwriting workflow.

The most effective insurers are not those with the most data, but those using data that is **trusted, actionable, and understood**. They are also applying that data consistently across the underwriting lifecycle, from initial triage through to portfolio management and reinsurance decisions.

This report explores how insurers can move from data abundance to decision clarity, and how a more focused approach to cyber risk data can support both underwriting performance and long-term portfolio resilience.

Key takeaways

- More cyber risk data does not automatically lead to better underwriting decisions
- Data must fit into the underwriting workflow to be useful
- Different risks require different data approaches and levels of scrutiny
- Single-risk insights increasingly influence portfolio-level outcomes
- The most effective approach is to start simple, validate impact, and specialize over time

The cyber risk data paradox

Over the past decade, cyber insurance underwriting has undergone a significant shift. Where underwriters once had limited external data, they now have access to a wide range of sources, including security perimeter telemetry, vulnerability data, breach intelligence, and third-party dependence risk indicators. At the same time, the number of data providers has grown, each offering different perspectives on cyber risk.

This expansion has created opportunity. It has also introduced complexity.

Underwriters are now faced with a new set of questions:

- Which data sources should be trusted?
- Which signals are relevant to insurance outcomes vs incentivising perfunctory fixes?
- How should this data be incorporated into underwriting decisions?
- How can meaningful insights be separated from noise?

The result is a paradox. More data has increased visibility into cyber risk, but it has also made decision-making more difficult.

> **More data has expanded the possibilities for cyber underwriting, but it has raised the bar for determining what is actually useful.**

At its core, this is not a data availability problem — it's about understanding how to turn the right data into the right decisions.

The real challenge: making data usable

The cyber insurance market does not need more data. It needs data that can be used consistently and confidently in underwriting decisions.

For data to be effective, it must meet three key criteria:

- **Trusted**

  Underwriters need confidence in both the source and relevance of the data. If a signal cannot be explained or validated, it is unlikely to be used or relied upon in decision-making.

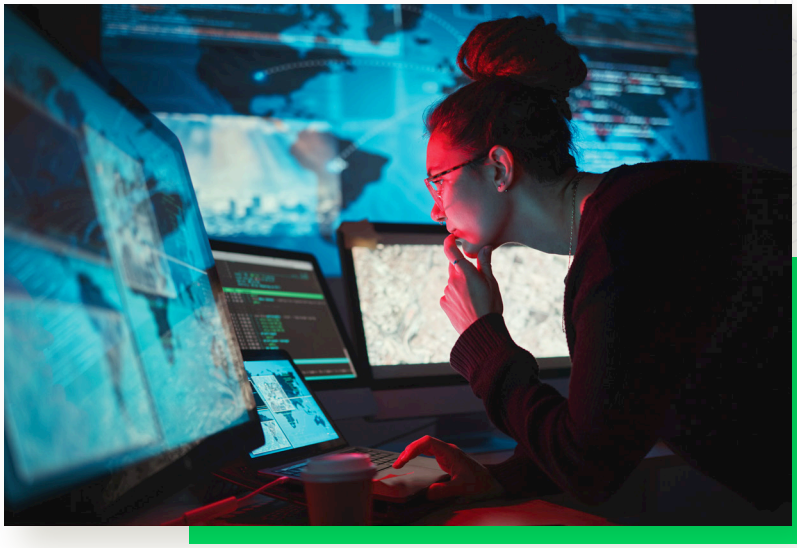
- **Actionable**

  Data must influence a decision. This could mean informing risk selection, triggering further investigation, supporting pricing adjustments, or guiding portfolio management. If it does not change an outcome, it adds little value.

- **Understood**

  Even technically strong data will not be adopted if it is not clearly explained. As new tools make it easier to synthesize fragmented signals, underwriters still need to understand what a signal represents, how it has been interpreted, and why it matters in an insurance context.

The question is no longer whether cyber risk data has a role in underwriting. It is whether that data is credible enough to trust, practical enough to act on, and clear enough to use consistently.



Where data creates value across the underwriting lifecycle

Cyber risk data should not be limited to supporting individual underwriting decisions. It should be used across the full insurance lifecycle:

Risk triage and selection

Data can help underwriters quickly assess new submissions, identify higher-risk accounts, and prioritize where to spend time. In lower-touch segments, it can also support more automated decision-making.

Risk assessment and pricing

Signals and insights can inform a deeper understanding of a company's security posture, exposure, and risk profile. This supports more consistent underwriting decisions and increasingly influences pricing models.

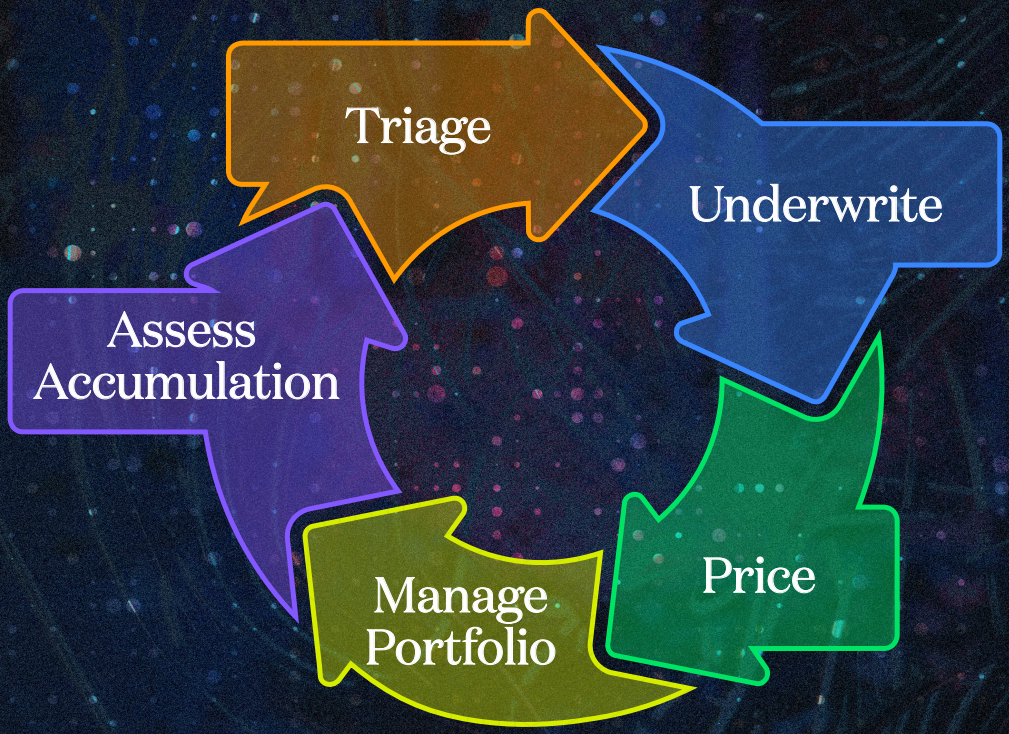
Portfolio management and book oversight

Portfolio managers are using data to assess overall book health, identify trends, and monitor how risk is evolving over time. This enables more informed decisions at a portfolio level, including feedback for risk triage and risk assessment at the point of underwriting.

Reinsurance and accumulation management

Reinsurers and carriers are using data to evaluate systemic exposure, understand concentrations, and assess potential adverse risk across portfolios. They, in turn, are able to provide feedback on what is driving losses in the market.

A connected workflow



This shift reflects a broader trend. Cyber underwriting is becoming more connected, with data flowing across functions rather than being used in isolation.

For decision-makers, this creates an opportunity to improve alignment between underwriting, actuarial, and portfolio management teams. For underwriters, it means data needs to be both accessible and usable within their day-to-day workflow.

Why one-size-fits-all data does not work

Not all risks are the same, so the data needed to evaluate them varies as well. There are different approaches for different types of risk:

Large and complex organizations

These companies often have extensive infrastructure, diverse operations, and significant regulatory exposure. Assessing them typically requires a broader set of data points to build a complete picture of risk.

However, more data also introduces more noise. The challenge is not just collecting data, but identifying which signals are most relevant.

Small and mid-sized organizations

Smaller companies often rely on cloud infrastructure and third-party providers. This can make traditional data collection methods less effective, as there is less visibility into their underlying systems.

In these cases, having less data is not necessarily a disadvantage. What matters is the reliability and relevance of the data that is available.

The role of industry, geography, and context

Cyber risk also varies significantly by industry, geography, and business model: A healthcare provider faces different risks than a manufacturing company, and a global enterprise operates under different regulatory pressures than a local business. Threat environments vary across regions. As a result, data should be interpreted within the context of the specific risk being assessed.

Better cyber underwriting does not come from broader data coverage, it comes from more context-specific insights. This shift toward specialization is already underway and is becoming a defining feature of how cyber risk data evolves.

From single-risk decisions to portfolio resilience

While much of the focus on cyber risk data is at the individual account level, its impact extends much further. Every underwriting decision contributes to the overall composition of a portfolio. Understanding individual risks is only part of the picture. Insurers also need to consider how those risks interact.

Key factors include:

- Technology dependencies and shared platforms
- Exposure to common vulnerabilities
- Patch management practices
- Backup capabilities
- Network segmentation

These elements influence not only the likelihood of individual incidents, but also the potential for systemic events and accumulation risk.

From insight to resilience

Stronger single-risk insights can support better portfolio construction, improved visibility into concentrations, more informed reinsurance decisions, and greater resilience to systemic events.

The goal is not perfect prediction at the account level — it is better-informed portfolio construction. This perspective helps align underwriting decisions with broader business objectives, including capital allocation, growth, and risk appetite.

The direction of travel: automation and specialization

The cyber insurance market is continuing to evolve, with increasing interest in automation and more efficient underwriting workflows. In certain segments, particularly small and mid-sized risks, more automated approaches are becoming viable. Data-enabled workflows can support faster decision-making and improve scalability.

At the same time, the market has not yet converged on a single standard for cyber risk data. Different carriers prioritize different signals, workflows, and approaches.

New technologies may make it easier to extract structure from fragmented or unstructured information, but insurers still need clear frameworks for deciding how those insights should be used.

The priority may be less about forcing every input into a common format, and more about creating consistent ways to interpret, validate, and apply diverse sources of data within underwriting decisions.

What this means in practice

- Automation will increase, especially in lower-touch segments
- Data will need to be easier to connect, interpret, and apply within underwriting workflows New technologies, including AI, may help insurers extract structure from fragmented and unstructured data sources
- Underwriters will continue to play a critical role in setting guidelines, validating outputs, and managing exceptions
- Automation does not remove the need for judgment. It changes how that judgment is applied.

The path ahead for insurers

For insurers looking to improve how they use cyber risk data, the path forward does not require a complete transformation. It requires a more focused and practical approach for improving data usage.

Insurers should start with data they will actually use, validate against their own experience, specialize over time and embed data into the workflow. This approach allows insurers to build capability progressively, without disrupting existing workflows.

Becoming a differentiator in an evolving market

Cyber risk data has become an essential component of modern underwriting. However, its value is not determined by volume, but by how effectively it supports decision-making.

Insurers that focus on data that is trusted, actionable, and understood — and that fits within their workflows — are better positioned to improve underwriting performance and build resilient portfolios.

As the market continues to evolve, the ability to turn data into clear, consistent decisions will become an increasingly important differentiator. Across the market, different approaches are emerging to address these challenges. Leading analytics providers are focusing on combining multiple data sources, validating signals against real-world outcomes, and presenting insights in a way that aligns with underwriting workflows. AI may accelerate this process, but the core requirement remains the same: insurers need outputs they can trust, explain, and act on.

CyberCube applies a multi-source approach to data, combining security, firmographic, event, and technology dependency insights to support underwriting and portfolio decisions. This type of approach reflects the broader direction of the market: moving from raw data toward curated, decision-focused insights.

If this is the future of cyber underwriting, it is not defined by having more data. It is defined by using the right data, in the right way.

CyberCube