TrendAI™ Research

A Data-Driven View of Cyber Risk Structure

How Attack Pressure and Exposure Shape Damage

Matsukawa Bakuei
Principal Threat Researcher, Forward-Looking Threat Research

Table of Contents

Executive summary

The central message is clear: cyber risk cannot be understood through any single indicator alone. The findings suggest that observed damage is shaped not only by how much attack pressure an organization faces, but also by how much exposure it has and how effectively harmful activity appears to be detected, contained, and limited once attacks occur. In that sense, cyber risk is better understood not as an isolated score or condition, but as a structured relationship among external pressure, organizational exposure, and the ability to limit harmful outcomes.

This study examines how attack pressure, exposure, and observed damage-related activity are associated across 2,014 enterprise-scale organizations worldwide that continuously used TrendAI Vision One™ Cyber Risk Exposure Management (CREM) and extended detection and response (XDR) throughout 2025. It also considers what those relationships may imply for exposure management and detection and response capability. In this study, Attack Pressure refers to the overall level of observed attack intensity measured by an organization's average Attack Index over the study period.

The analysis showed that Attack Pressure had the strongest observed relationship with Damage. At the same time, Exposure—defined in this study as the level of risk based on vulnerabilities, misconfigurations, and exposed services—became more important under harsher attack conditions. Organizations facing both high Attack Pressure and high Exposure showed substantially higher Damage than those with low levels of both. These results suggest that risk is not defined by the attack environment alone. It is shaped by how Attack Pressure, Exposure, and damage constraint interact in practice.

The analysis also showed that industry is useful for understanding broad risk tendencies, especially differences in Attack Pressure. However, substantial variation remained even within the same industry, which means industry context is informative, but not sufficient to explain the risk faced by any individual organization. Similar organizations may still experience different outcomes depending on their exposure conditions and the extent to which harmful activity appears to be constrained in practice.

This perspective is valuable not only analytically, but also operationally. It provides a more interpretable view of why outcomes differ, making cyber risk easier to assess, explain, and prioritize in practice. For security leaders and other decision-makers, the implication is straightforward: the Cyber Risk Index (CRI) provides a useful summary view of cyber risk, but its practical value increases when organizations also understand what drives that risk—whether it is the surrounding attack environment, the exposure that amplifies it, or the extent to which harmful activity appears to be constrained in practice.

Key takeaways

1. **Attack Pressure and Exposure together were associated with up to a 3.3-fold difference in observed Damage, with an approximately 30% gap under high Attack Pressure.**

Organizations with both low Attack Pressure and low Exposure averaged approximately 2.9 Damage Months (defined in this study as the number of months in which later-stage attack activity was observed in an organization's telemetry), while those with both high Attack Pressure and high Exposure averaged approximately 9.6 Damage Months. Under high Attack Pressure, organizations with lower Exposure showed about 30% fewer Damage Months than those with higher Exposure. In addition, the correlation between Attack Pressure and Damage Months was 0.545, the strongest among the three relationships examined in this study. Together, these results show that Attack Pressure was the strongest overall signal associated with observed Damage, while Exposure became more consequential under harsher attack conditions.

2. **Industry helps explain broad risk tendencies, but not the full risk of any individual organization.**

At the industry group level, average differences in Exposure were relatively limited, while clearer differences appeared in average Attack Pressure. This indicates that industry can be a useful lens for understanding broad differences in attack environment. At the same time, organizations within the same industry still showed substantial variation in both Attack Pressure and Exposure, indicating that cyber risk is formed more directly at the organizational level.

3. **Differences in Damage are not explained by risk environment alone.**

The findings suggest that differences in observed Damage are associated not only with Attack Pressure and Exposure, but also with how effectively harmful activity is limited in practice. To organize this relationship in a practical way, this study introduces a Cyber Risk Positioning Map that combines the CRI with a supplementary Detection & Response Capability Score. This map is not a predictive model, but a practical framework for relative comparison, interpretation, and prioritization.

1

Introduction

Why do similar organizations experience different levels of damage?

Even within the same industry, organizations of comparable size and with broadly similar IT environments do not always experience the same level of harmful activity or business impact. In some cases, attacks are frequently observed and lead to persistent damage-related activity. In others, serious damage remains limited even though the organizations operate under broadly similar conditions.

This raises a fundamental question: why do organizations that appear broadly similar experience different levels of damage? Put differently, the issue may not be only how much attack activity organizations face, but also how the conditions around that activity shape whether it develops into more persistent harmful outcomes. In that sense, this may not be simply a question about attack volume, but about how different elements of cyber risk are structured and how they interact.

Cyber risk cannot be understood through any single indicator alone.

Why Attack Pressure alone may not explain Damage

Cyber damage is often discussed in relation to the amount of attack activity an organization faces. This is a reasonable starting point. In general, organizations exposed to more attack activity would be expected to face a greater chance of harmful outcomes.

However, whether Attack Pressure alone is sufficient to explain Damage remains an open question. In practice, some organizations operating under high Attack Pressure show relatively limited Damage, while others experience substantial Damage even when the Attack Pressure they face is not especially high. This raises the possibility that the relationship between attack activity and Damage may not be explained by Attack Pressure alone.

If so, the question is not whether Attack Pressure matters, but whether it is enough. The observed differences in Damage may instead reflect the influence of additional conditions—including organizational exposure—that shape how attack activity develops once it reaches an organization.

Exposure as an additional element of risk structure

One important factor is organizational exposure. Vulnerabilities, misconfigurations, and externally exposed services can increase the likelihood that attacks will succeed once they reach an organization. In this sense, exposure is a condition that influences how easily attack activity translates into harmful outcomes.

This perspective is consistent with the broader work of TrendAI™ on proactive security. In the December 2024 report, Reducing Ransomware Risk Through Proactive Attack Surface Management: Enabling Proactive Cybersecurity, TrendAI™ Research highlighted the importance of continuously reducing exposure-related risk through CREM. In a July 2025 report, Proactive Security: The Role of Exposure Management and Detection & Response Capability, TrendAI™ Research argued that exposure management and detection and response should be understood together when evaluating organizational cyber risk.

The issue may not be only how much attack activity organizations face, but also how the conditions around that activity shape whether it develops into more persistent harmful outcomes.

The present study builds on that line of work by extending it into a single analytical framework. Earlier work established two related points: the importance of reducing exposure, and the need to understand exposure management together with detection and response capability. This study examines how those conditions relate to observed Damage when Attack Pressure is also considered. In doing so, it asks whether cyber damage is better understood not through isolated indicators alone, but through the way multiple conditions interact in practice.

Purpose of this study

To better understand the structure of cyber damage, this study examines the relationships among the following three elements:

- Attack Pressure is the overall level of observed attack intensity an organization faced during the study period, represented in this study by its average Attack Index.

- Exposure is the level of organizational exposure associated with vulnerabilities, misconfigurations, and exposed services.
- Damage is the observed damage-related activity identified in later-stage attack behavior.

The goal of this study is not to explain Damage through any single factor. Rather, it is to examine whether Damage is better understood as the result of multiple interacting elements. Specifically, this study analyzes how the combination of observed attack activity and exposure conditions is associated with the occurrence and persistence of Damage, and considers whether this approach provides a more useful way to interpret cyber risk in practice.

2

Data and methodology

Dataset

This study used telemetry data aggregated in TrendAI Vision One™ over the one-year period from January through December 2025. The dataset included security-related observations derived from CREM and XDR. To ensure consistency in the analytical population, this study selected organizations that met the following criteria:

- Continuously used CREM and XDR throughout 2025
- Continuously used endpoint sensors throughout 2025
- Had from 500 to 10,000 employees

The dataset was limited to organizations with 500 to 10,000 employees to ensure consistent data quality and analytical comparability. Organizations outside this range are at the extreme ends of employee counts and tend to differ significantly in IT complexity and security maturity, which would make cross-group comparisons less reliable.

Applying these criteria resulted in a study population of 2,014 enterprise-scale organizations worldwide.

The purpose of these selection criteria was to reduce differences caused by inconsistent product usage or large differences in organizational scale. By focusing on organizations with continuous usage over the full year, this study aimed to improve comparability across organizations and to make the observed relationships among the metrics more interpretable.

Definition of metrics

To examine the structure of cyber risk, this study used three organization-level metrics derived from aggregated telemetry data: Attack Index, Exposure Index, and Damage Months. These metrics were selected to represent three distinct but related dimensions of cyber risk: attack pressure, exposure, and observed damage-related activity.

In this study, Attack Pressure refers to the overall level of observed attack intensity measured by an organization's average Attack Index over the study period. The study used Exposure Index as the indicator of organizational exposure and Damage Months as the indicator of observed damage-related activity.

TrendAI Vision One™ Cyber Risk Exposure Management (CREM) also calculates the Cyber Risk Index (CRI), which integrates multiple elements including Attack Index and Exposure Index. However, the core analysis in this study examines Attack Index, Exposure Index, and Damage Months separately to clarify how these elements are related to one another. In later sections, the CRI is used as a practical summary indicator for organizing the broader risk environment.

Attack Index

In this study, Attack Pressure refers to the overall level of observed attack intensity an organization faced during the study period, measured by its average Attack Index—a metric calculated from the types and volume of attack-related events observed against an organization.

Each organization's annual average Attack Index represents the overall level of Attack Pressure it faced in 2025.

Exposure Index

In this study, Exposure refers to the level of risk associated with an organization's attack surface, measured by its average Exposure Index—a metric calculated based on information such as vulnerabilities, misconfigurations, and externally exposed services.

Each organization's annual average Exposure Index represents its overall level of Exposure in 2025.

Damage Months

In this study, Damage Months represents observed damage-related activity, calculated by counting the number of months in which attack activity associated with the following MITRE ATT&CK™ tactics was observed in XDR telemetry within TrendAI Vision One™.

- TA0010 (Exfiltration)
- TA0040 (Impact)

These tactics are positioned in the later stages of the MITRE ATT&CK framework and are more likely to be associated with actions related to the occurrence or escalation of damage.

Damage Months does not directly measure the severity of financial, operational, or business impact. Rather, it is used as a proxy indicator representing the persistence of observed damage-related activity over time.

Analytical approach

This study examined the relationships among Attack Index, Exposure Index, and Damage Months at the organization level. The analysis was designed to address three questions:

1. Is higher Exposure associated with higher Attack Pressure?
2. Is higher Attack Pressure associated with more observed damage-related activity?
3. Is higher Exposure associated with more observed damage-related activity?

To address these questions, the study compared the distributions of Attack Index and Damage Months across grouped ranges of Exposure Index and Attack Index. For these pairwise grouped comparisons, the metrics were examined using predefined ranges to make broad distributional differences easier to interpret. Pearson correlation coefficients were also used to summarize the strength and direction of the relationships among the three metrics.

In addition, to examine how Attack Pressure and Exposure jointly relate to Damage, this study classified Attack Index and Exposure Index into four levels each and compared average Damage Months across their combinations. These four levels were defined using quartiles of the organization-level annual average values for each metric. This approach made it possible to assess whether damage levels differ meaningfully depending on the combination of Attack Pressure and Exposure, rather than treating each factor in isolation.

Finally, the study extended the analysis to industry groups to examine how these relationships appear at a broader sector level and how much variation remains at the organizational level within the same industry.

Scope and interpretation

Several points are important for interpreting the results. First, this study analyzes associations among metrics derived from observed telemetry data. It does not establish causal relationships.

Second, Damage Months is a proxy indicator based on observed later-stage attack behavior and should not be interpreted as a direct measure of financial loss, operational disruption, or incident severity.

Third, the purpose of this analysis is not to build a predictive model, but to better understand the structure of cyber risk by examining how attack pressure, exposure, and observed damage-related activity are related in practice.

For these reasons, the findings of this study should be interpreted as an empirical view of how these elements are associated within the observed population, rather than as a complete explanation of all factors that shape cyber damage.

3

Overall trends in cyber damage

Relationships among Attack Pressure, Exposure, and Damage

This study first examined how Attack Pressure, Exposure, and Damage are related across the full population of organizations. To clarify the overall structure of cyber damage, the analysis focused on three pairwise relationships: Exposure and Attack Pressure, Attack Pressure and Damage, and Exposure and Damage. Examining these relationships separately makes it possible to understand how each element relates to the others before considering their combined effects.

The relationship between Exposure and Attack Pressure

The first question was whether greater organizational Exposure is associated with higher Attack Pressure. To examine this relationship, this study divided the Exposure Index into grouped ranges and compared the distribution of the Attack Index across those ranges.

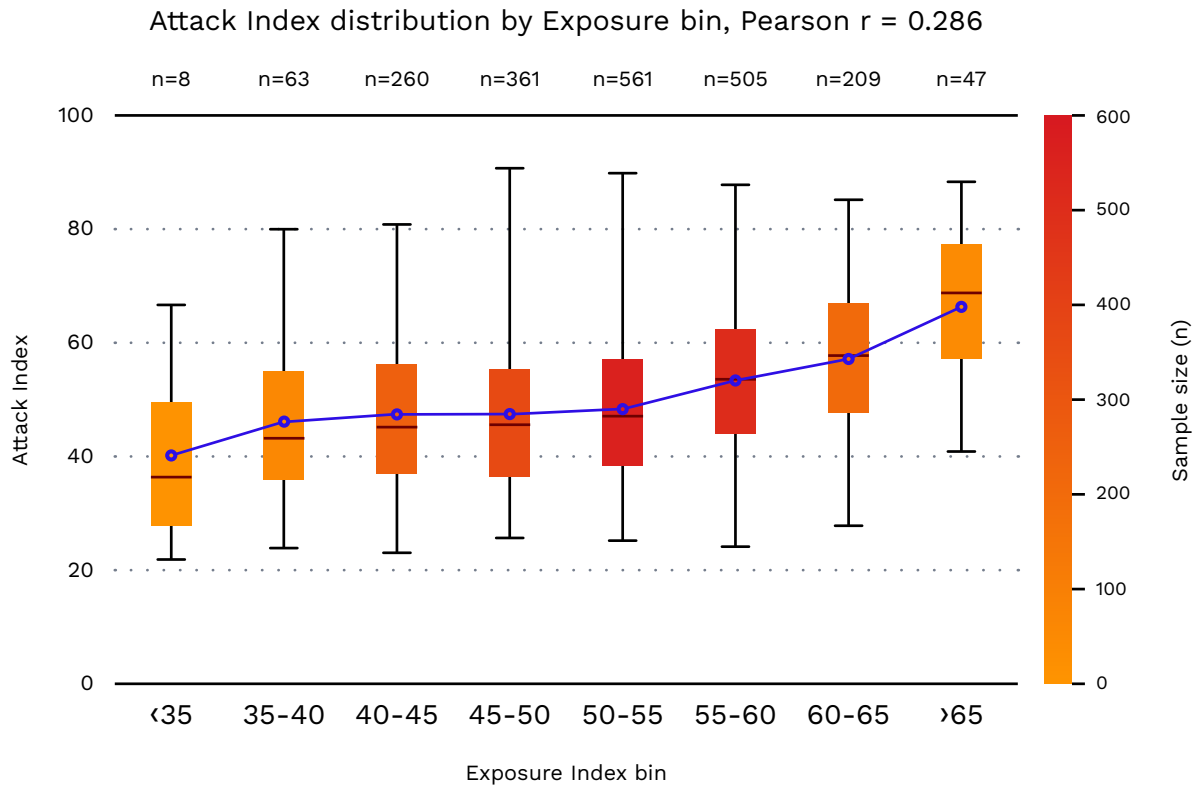

Figure 1. Distribution of Attack Index across Exposure Index ranges

The Pearson correlation coefficient between the Exposure Index and the Attack Index was r = 0.286, indicating a weak positive relationship. On average, organizations with higher Exposure tended to face higher Attack Pressure.

At the same time, the relationship was not strong. Even within the same exposure range, the Attack Index varied substantially across organizations. This indicates that Exposure alone does not determine Attack Pressure. Rather, Attack Pressure appears to reflect not only the degree of Exposure, but also other factors such as industry, region, organizational visibility, and attacker targeting preferences.

Viewed practically, this suggests that Exposure is one condition that can make attack activity more likely to reach an organization, but it does not by itself explain how much Attack Pressure that organization will face.

The relationship between Attack Pressure and Damage

The second question was whether higher Attack Pressure is associated with more observed damage-related activity. To examine this relationship, this study divided the Attack Index into grouped ranges and compared the distribution of Damage Months across those ranges.

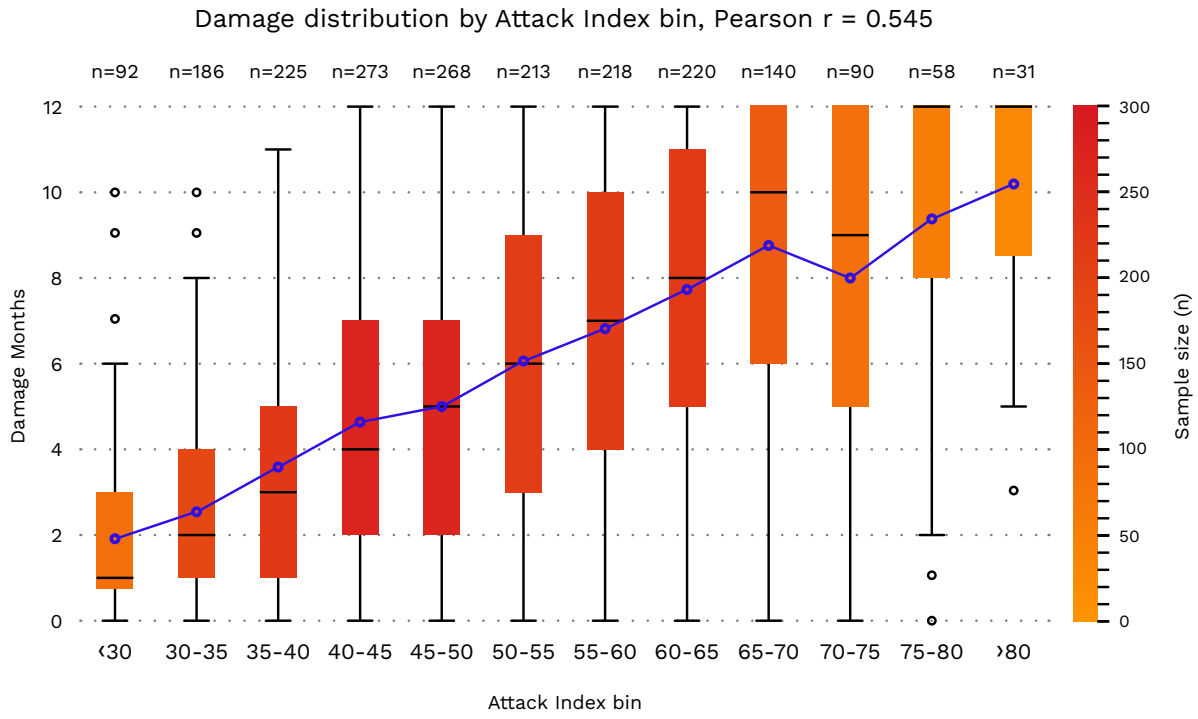

Figure 2. Damage Months distribution across Attack Index ranges

The Pearson correlation coefficient between Attack Index and Damage Months was r = 0.545, the strongest among the three pairwise relationships examined in this study. This indicates a moderate positive relationship: organizations facing higher Attack Pressure tended, on average, to show more Damage Months.

The overall pattern is clear. As the Attack Index increased, both the average level and the central tendency of Damage Months increased. This suggests that Attack Pressure is the strongest single factor associated with observed Damage in this dataset.

At the same time, substantial variation remained within the same Attack Index ranges. Even among organizations exposed to similarly high Attack Pressure, some showed relatively limited Damage Months while others showed much higher values. This indicates that Attack Pressure is highly informative, but not sufficient on its own to explain differences in observed Damage.

Taken together, these results show that Attack Pressure has the clearest relationship with Damage among the three metrics examined here. However, the remaining variation also suggests that additional factors influence how far attack activity develops into persistent damage-related activity in practice.

The relationship between Exposure and Damage

The third question was whether greater Exposure is associated with more observed damage-related activity. To examine this relationship, this study divided the Exposure Index into grouped ranges and compared the distribution of Damage Months across those ranges.

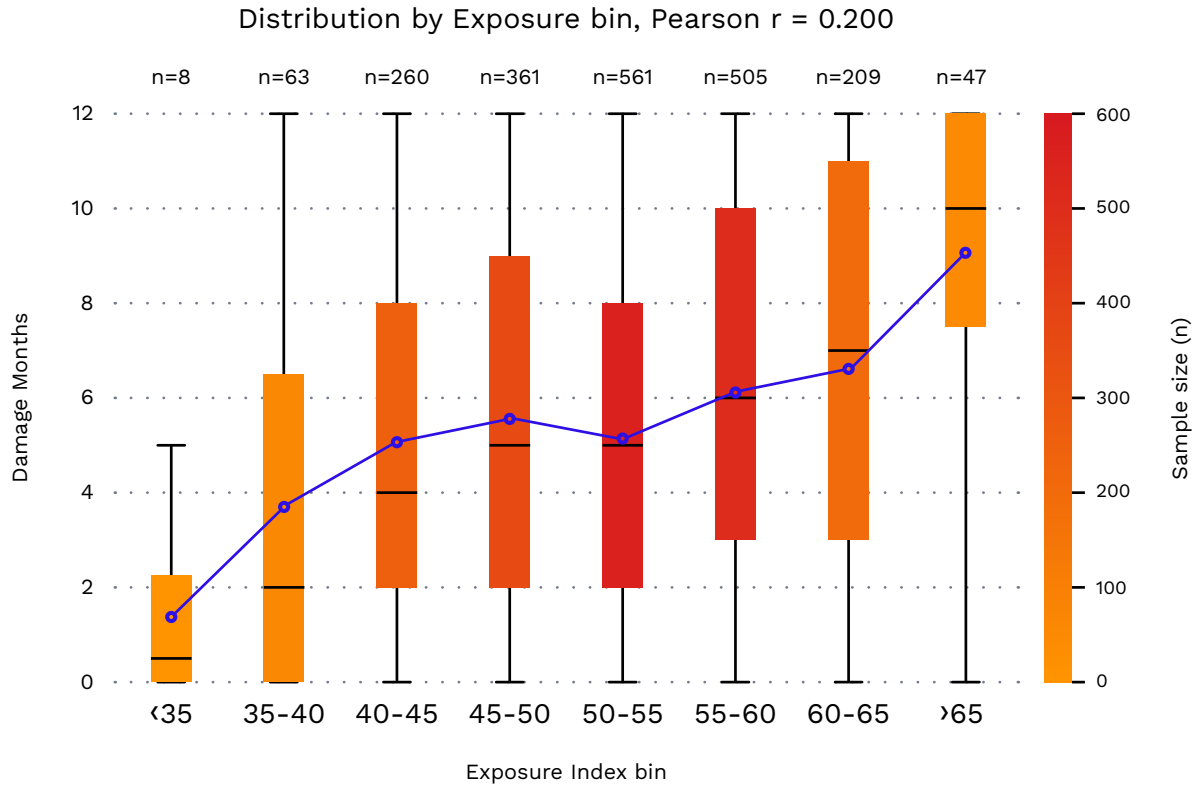

Figure 3. Damage Months distribution across Exposure Index ranges

The Pearson correlation coefficient between Exposure Index and Damage Months was r = 0.200, indicating a weak positive relationship. On average, organizations with higher Exposure tended to show somewhat more Damage Months, but the relationship was limited.

The figure also shows substantial variation in Damage Months within the same Exposure ranges. Some organizations with relatively high Exposure showed limited Damage Months, while some with less elevated Exposure still showed relatively high values. This indicates that Exposure alone does not adequately explain observed Damage.

At the same time, the weaker direct relationship should not be interpreted to mean that Exposure is unimportant. Rather, it suggests that Exposure is less informative when viewed in isolation than when viewed in the context of Attack Pressure. Exposure becomes more meaningful when explaining why organizations operating under harsher attack conditions still experience different levels of Damage.

Conceptually, the observed pattern may be summarized as follows:

Exposure → Attack Pressure → Damage

This is not a causal model. Rather, it is a simple way to summarize the structure observed in the data: Exposure is weakly associated with Attack Pressure, and Attack Pressure is more strongly associated with Damage.

Taken together, these results indicate that Exposure is an important part of cyber risk, but its practical meaning becomes clearer when it is considered together with Attack Pressure rather than on its own.

Exposure becomes more meaningful when explaining why organizations operating under harsher attack conditions still experience different levels of damage.

A structural view of cyber damage

The relationships examined above reveal a clear overall structure. Among the three pairwise relationships, Attack Pressure showed the strongest observed relationship with Damage Months, while the direct relationship between Exposure and Damage Months was weaker. This indicates that observed Damage is not best understood through Exposure alone, but neither is it adequately explained by Attack Pressure alone. A more useful interpretation is to examine how Attack Pressure and Exposure operate together.

Relationship	Correlation	Interpretation
Exposure and Attack Pressure	0.286	Weak positive relationship
Attack Pressure and Damage	0.545	Moderate positive relationship
Exposure and Damage	0.200	Weak positive relationship

Table 1. A summary of pairwise correlations among Exposure, Attack Pressure, and Damage

Table 1 summarizes the observed pairwise correlations. Attack Pressure and Damage showed the strongest relationship, indicating that differences in the surrounding attack environment were closely associated with differences in observed damage-related activity. By contrast, the weaker direct relationship between Exposure and Damage suggests that Exposure is not equally informative under all conditions. Its practical meaning becomes clearer when it is interpreted together with Attack Pressure rather than in isolation.

To examine that joint structure, this study classified Attack Index and Exposure Index into four levels each and compared average Damage Months across all sixteen combinations.

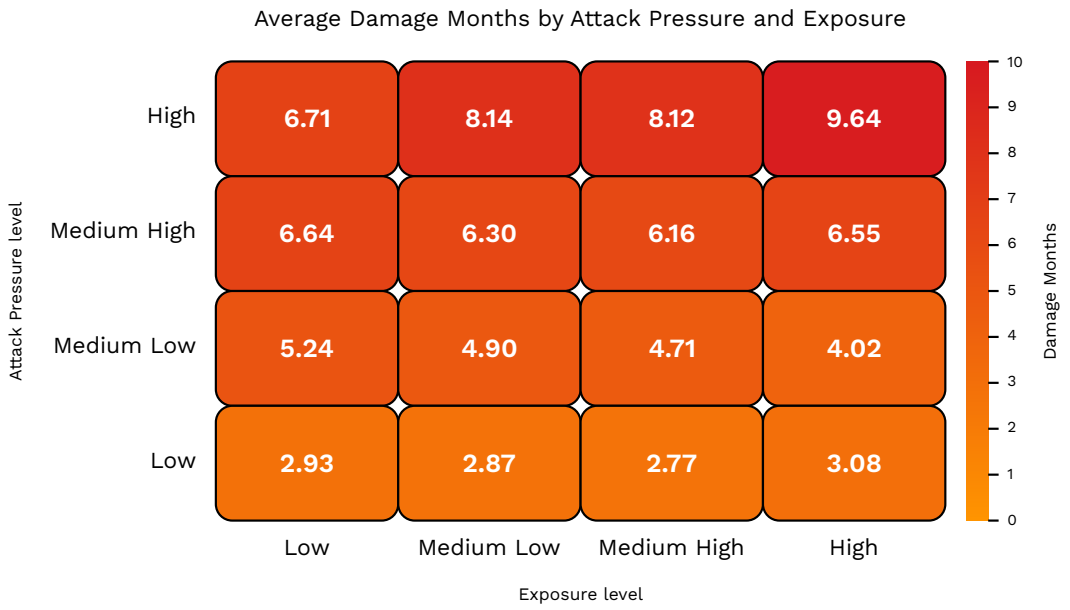

Figure 4. Average Damage Months by Attack Pressure and Exposure combinations

Figure 4 shows the overall 4×4 structure. Across the full grid, organizations in the lowest Attack – Exposure segment averaged approximately 2.93 Damage Months, while those in the highest Attack – Exposure segment averaged approximately 9.64 Damage Months. This represents an approximately 3.3-fold difference. An equally important pattern appears within the highest Attack Pressure conditions. Among organizations in the highest Attack Pressure segment, those in the lowest Exposure segment averaged approximately 6.71 Damage Months, compared with approximately 9.64 in the highest Exposure segment. This corresponds to an approximately 30% lower level of observed damage-related activity under the same high-attack conditions. In other words, Exposure became materially more informative when organizations were already operating in a harsher attack environment.

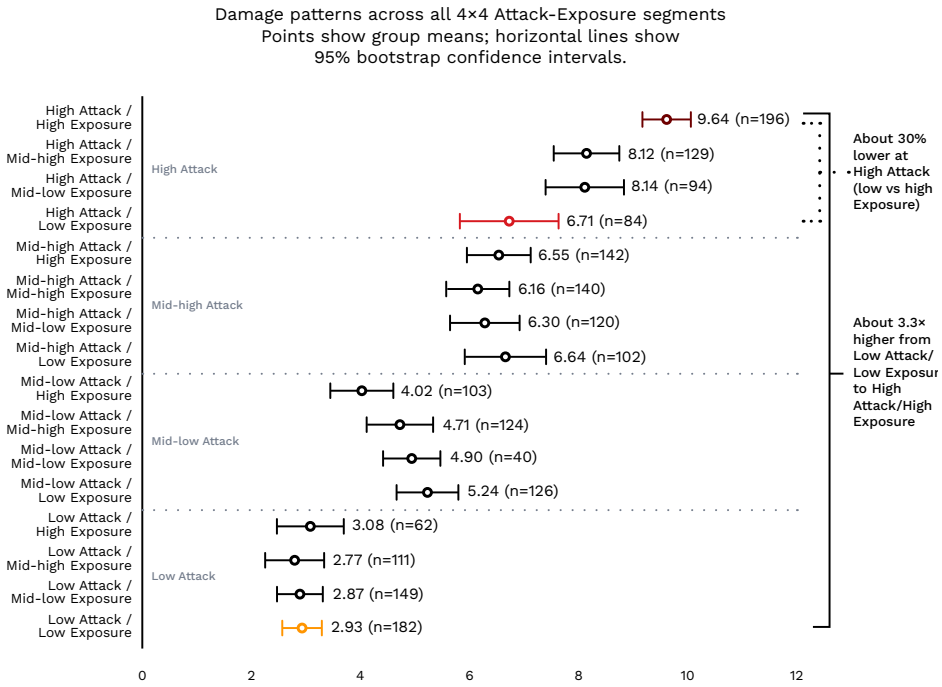

Figure 5. The Damage patterns across all 4×4 Attack – Exposure segments with 95% bootstrap confidence intervals

Figure 5 adds confidence intervals to the same 4×4 framework. It highlights the same two key contrasts: the approximately 3.3-fold difference between the lowest and highest Attack – Exposure segments, and the approximately 30% gap between the groups with the lowest and highest Exposure within the highest Attack segment. These differences remain clear in the confidence-interval view, reinforcing that the observed structure is robust enough to support practical interpretation.

This pattern is one of the most important findings in the study. Exposure does not contribute to Damage in a uniform way across all environments. Under lower Attack Pressure conditions, differences in Exposure were associated with relatively smaller differences in Damage Months. Under higher Attack Pressure conditions, however, the separation became much clearer. This makes Exposure important not as an isolated risk signal, but as a factor that helps explain why similarly targeted organizations may still experience meaningfully different levels of persistent damage-related activity.

Additional robustness checks supported the same interpretation. In supplementary analyses, including rank-based comparisons, the direction of the key relationships remained consistent, supporting the stability of the result. At the same time, the figures also show that Damage does not collapse into a single level even within the same broad Attack – Exposure conditions. Meaningful variation remains across organizations operating under similar levels of Attack Pressure and Exposure.

From a conceptual perspective, the observed structure may be summarized as follows:

$$\textbf{Damage} \approx \frac{\textbf{Attack Pressure} \times \textbf{Exposure}}{\textbf{Detection \& Response Capability}}$$

This is not a statistically estimated formula. Rather, it is a simple conceptual expression of the pattern observed in the data: Damage tends to rise as Attack Pressure and Exposure increase, but it may remain more limited where harmful activity appears to be constrained more effectively in practice.

Taken together, these results support a more structured interpretation of cyber damage. Attack Pressure provides the strongest overall signal. Exposure becomes more informative under harsher attack conditions. Even after both factors are considered together, meaningful variation remains. Cyber damage is, therefore, better understood not as the result of any single metric, but as the outcome of multiple interacting conditions.

From a practical perspective, the implication is clear. Organizations should not interpret cyber risk only through the amount of attack activity they face, nor only through Exposure viewed in isolation. The key question is how Attack Pressure and Exposure combine to shape the likelihood that harmful activity will persist. This perspective provides the foundation for the more practical risk-management and positioning framework introduced in the following chapters.

4

Overview of industry-specific cyber risk

Definition of industry groups

To examine how cyber risk structures differ across industries, this study grouped organizations into broader industry groups. In TrendAI Vision One™ telemetry data, organizations are originally classified into more detailed industry categories. However, using those categories directly would result in too many groups for clear comparison and would reduce interpretability at the industry level. For that reason, this study aggregated the original categories into six broader industry groups. The aggregation shown in Table 2 should be understood as a practical analytical simplification to support comparison at a broader level, not to eliminate meaningful differences within each group.

Industry Group	Included Industry Categories
Financial	Financial Services, Insurance
Healthcare	Healthcare, Pharmaceuticals
Technology, Media, and Communications	Technology, Telecommunications, Entertainment, Communications
Industrial and Energy	Agriculture, Construction, Energy, Manufacturing, Transportation, Utilities
Public Sector	Government and Public Services, Education, Defense
General Market	Other industries

Table 2. The category composition of each industry group

Industry cyber risk landscape

To visualize how cyber risk structures differ across industries, this study constructed an industry cyber risk landscape, shown in Figure 6. This figure represents each industry group using the mean values of Attack Index, Exposure Index, and Damage Months for the organizations included in that group.

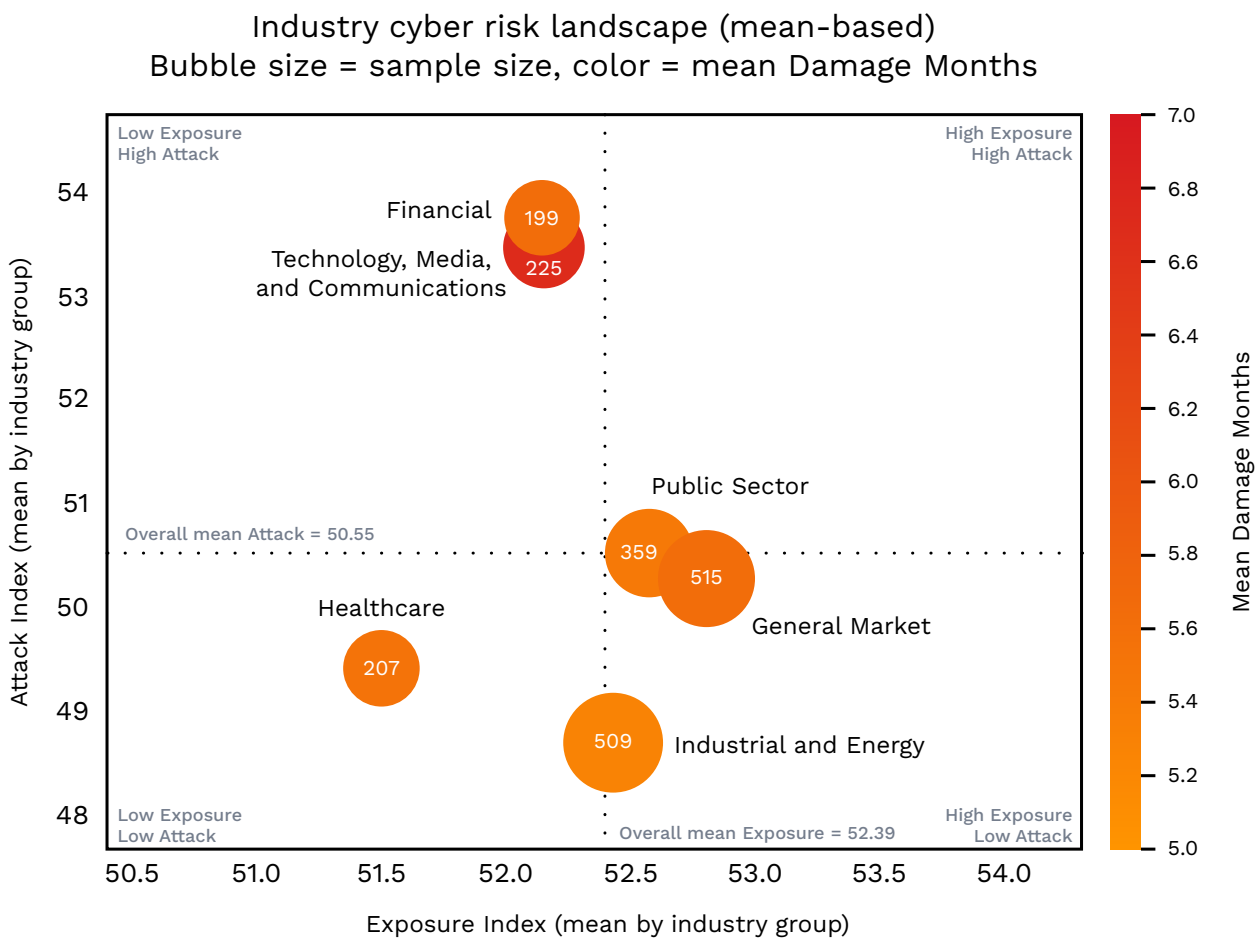

Figure 6. The industry cyber risk landscape

In Figure 6, the horizontal axis represents the mean Exposure Index and the vertical axis represents the mean Attack Index. The bubble size represents the number of organizations in each industry group, and the color represents the mean Damage Months. Dashed lines indicate the overall mean values of Exposure Index and Attack Index and divide the figure into four quadrants.

The purpose of this figure is not to describe the full distribution within each industry, but to provide a broad comparative view of how industries are positioned relative to one another. For this reason, mean values were used as indicators of the approximate center of gravity of each industry group.

Viewed in this way, the figure provides a compact summary of industry-level cyber risk environments from three perspectives: Exposure, Attack Pressure, and observed damage-related activity.

Industry-level risk structures

The industry cyber risk landscape shows that cyber risk structures differ across industries, but the magnitude of those differences is not the same across all metrics. Differences in mean Exposure Index were relatively small across industries, whereas clearer differences appeared in mean Attack Index and, to a lesser extent, in mean Damage Months.

The mean values used to construct Figure 6 are shown in Table 3.

Industry Group	Sample size	Exposure Index mean	Attack Index mean	Damage Months mean
Industrial and Energy	509	52.42	48.72	5.29
Healthcare	207	51.49	49.43	5.55
General Market	515	52.80	50.30	5.65
Public Sector	359	52.57	50.54	5.46
Technology, Media, and Communications	225	52.15	53.49	6.72
Financial	199	52.14	53.77	5.66

Table 3. The mean Exposure Index, Attack Index, and Damage Months by industry group

The overall mean values across all organizations were as follows:

- Overall mean Exposure Index = 52.39
- Overall mean Attack Index = 50.55

Two broad patterns stand out. First, the mean Exposure Index values were tightly clustered, ranging from 51.49 to 52.80. This indicates that differences in average Exposure across industries were limited in this dataset. Second, the mean Attack Index values varied more clearly, ranging from 48.72 to 53.77. This suggests that industry-level differences were more visible in Attack Pressure than in Exposure.

These patterns indicate that industry is more useful for understanding broad differences in attack environment than for explaining average Exposure levels. Exposure appears to be shaped more strongly by organization-specific conditions than by industry alone. The following points summarize observations from the data:

- The Financial group operated in a comparatively severe attack environment, but its observed damage-related activity remained closer to the middle of the industry distribution. From a comparative perspective, this may indicate that high Attack Pressure does not necessarily translate into the highest observed Damage.
- The Technology, Media, and Communications group occupied a position similar to the Financial group in terms of both Attack Index and Exposure Index, yet its Damage Months mean was clearly higher. This suggests that even when industries are exposed to similarly high Attack Pressure and broadly similar average Exposure, their observed Damage outcomes may still differ.
- The Public Sector group was positioned close to the overall mean on both major axes. This positioning suggests that the group represents a relatively average industry-level risk structure within this dataset. It does not stand out as especially high or especially low in either Exposure or Attack Pressure at the mean-value level.
- The General Market group showed more Exposure on average, but Attack Pressure was not especially elevated.
- The Healthcare group showed relatively lower mean values for Attack Pressure and Exposure at the industry group mean level in this dataset. Although organizations in the Healthcare group have often been associated with prominent reported incidents, the broader average pattern observed here was more moderate than those cases alone might suggest.
- The Industrial and Energy group showed a relatively lower Attack Pressure and Damage profile at the group mean level. Within this dataset, Industrial and Energy appeared less elevated than the other groups in terms of both observed Attack Pressure and observed damage-related activity.

Key patterns observed across industries

Taken together, the industry-level analysis reveals three important patterns.

First, differences in average Exposure across industries were limited. The mean Exposure Index values were tightly clustered, suggesting that Exposure, at least at this aggregated level, did not vary dramatically by industry. One likely reason is that Exposure is strongly influenced by organization-specific conditions such as system configuration, vulnerability status, and externally visible assets. As a result, variation within each industry may be substantially greater than what the averages suggest.

Second, differences in Attack Pressure were more visible than differences in Exposure. The Financial group and the Technology, Media, and Communications group were positioned on the higher Attack Pressure side, whereas Industrial and Energy and Healthcare were positioned on the lower Attack Pressure side. This suggests that industry may be more informative for understanding broad differences in attack environment than for understanding average Exposure.

Third, similar levels of attack pressure did not always correspond to similar levels of observed damage. The most notable comparison is between the Financial and Technology, Media, and Communications. These two groups had nearly the same average Attack Index and broadly similar average Exposure Index, yet Technology, Media, and Communications showed clearly higher mean Damage Months. This indicates that even under broadly similar external conditions, observed damage-related activity may still differ by industry group.

Taken together, these patterns suggest that industry is useful for identifying broad differences in cyber risk environment, especially in Attack Pressure. At the same time, industry averages alone are not sufficient to explain how much observed Damage is associated with each group.

Industry as a useful but incomplete lens

The findings in this chapter suggest that industry is a useful lens for understanding cyber risk, but only at a broad level. Industry-level averages help reveal general differences in Attack Pressure and provide a compact way to position sectors relative to one another. However, the relatively small differences in average Exposure and the remaining differences in observed Damage indicate that industry alone does not provide a complete explanation of cyber risk.

For that reason, industry should be understood as a starting point for interpreting the risk environment, not as a substitute for organization-level analysis. The next chapter turns from industry means to organizational distributions within each industry to examine how much variation remains among organizations that belong to the same sector.

5

Organizational differences within the same industry

Variation within industries

Industry averages alone do not capture how widely organizations are distributed within the same sector. Even when an industry group appears to occupy a relatively clear position at the mean level, the organizations within that group may still be spread across very different risk environments.

Industry creates tendencies, but risk is formed at the organizational level.

To examine this point, this study plotted individual organizations by Exposure Index and Attack Index and compared their distributions across industry groups. Figure 7 shows the distribution of organizations within each industry group, where each point represents one organization. The horizontal axis shows the Exposure Index, the vertical axis shows the Attack Index, and color represents Damage Months. The blue X marks indicate the mean position of each industry group, and dashed blue lines indicate the overall mean Exposure Index and Attack Index values.

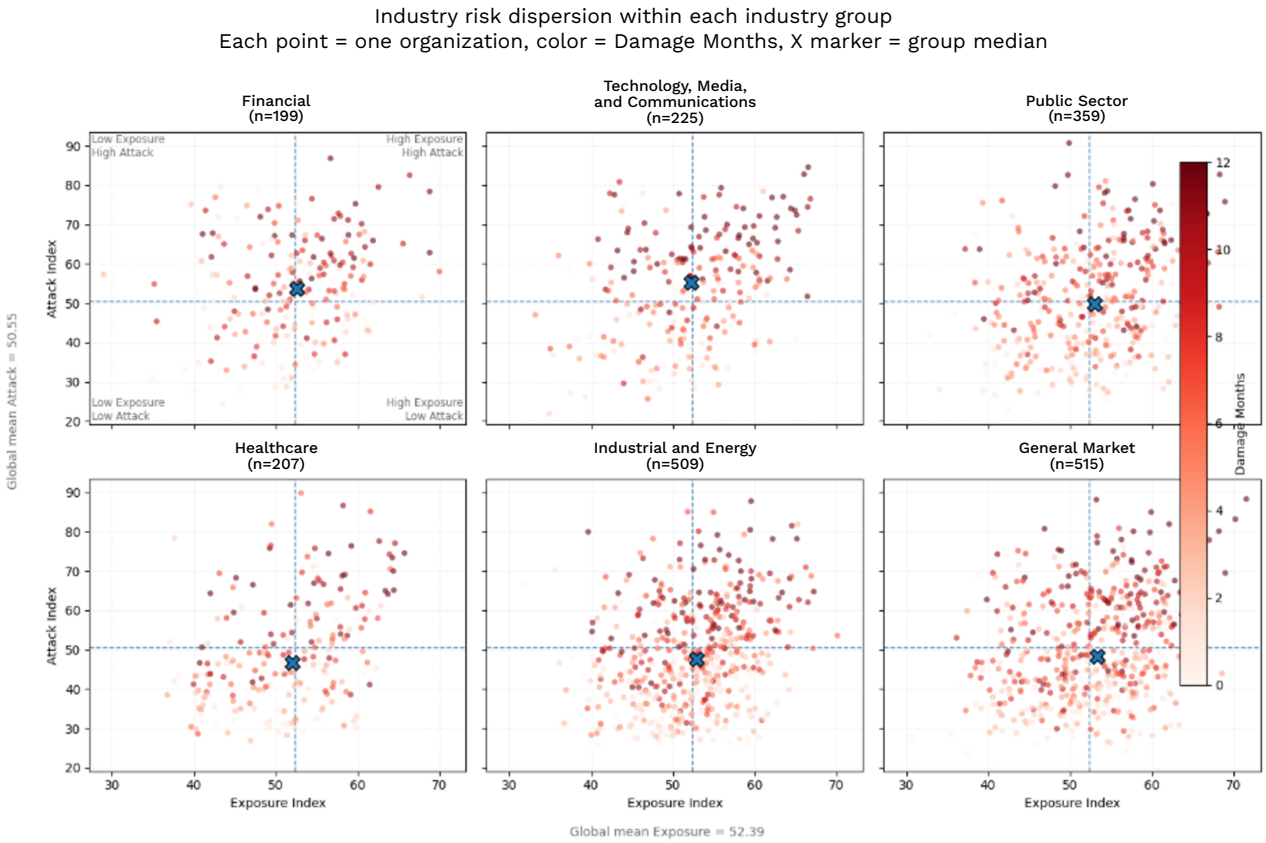

Figure 7. The organizational distribution within industry groups

Organizations within the same industry were widely dispersed rather than concentrated in a single area, which indicates that industry does not determine organizational

cyber risk in a simple or uniform way. Industry averages are useful for identifying broad tendencies, but they do not describe the full range of risk conditions faced by organizations within the same sector.

The mean position of an industry group can sometimes also obscure the internal spread of its organizations. A group whose average appears close to the center of the figure may still include organizations located in much higher- or lower-risk areas. Conversely, a group positioned in a relatively high-risk area on average may still include organizations operating under less severe conditions.

Taken together, industry-level averages provide useful context, but they should be complemented by organization-level analysis to understand how risk is distributed within each industry.

Why do differences appear even within the same industry?

The broad dispersion observed in Figure 7 raises an important question: Why do organizations within the same industry still differ so substantially in their levels of Attack Pressure and Exposure?

This study does not directly test the specific drivers of that variation. However, several factors may plausibly contribute to the differences observed within the same industry. The purpose of this section is not to identify those factors conclusively, but to provide a practical interpretation of why industry-level averages alone are not sufficient.

One possible factor is variation in organizational characteristics. Even within the same industry, organizations can differ substantially in business scale, digital footprint, brand visibility, strategic importance, and the kinds of data or systems they operate. These differences may affect how attractive an organization appears to attackers and how much attack activity it observes.

A second factor is variation in exposure structure. The Exposure Index reflects vulnerabilities, misconfigurations, and externally exposed services, all of which can differ greatly even among organizations in the same sector. Differences in cloud usage, internet-facing systems, vulnerability management practices, and system complexity may all affect how much exposure an organization presents.

A third factor is variation in regional operating context. Organizations in the same industry may still operate under different regulatory environments, infrastructure

conditions, geopolitical contexts, and attacker ecosystems depending on country or region. These differences may influence both attack pressure and exposure conditions.

A fourth factor may be variation in security operations and defensive capability. Even when organizations face broadly similar Attack Pressure and Exposure, they may differ in how effectively they detect, investigate, and contain harmful activity. This does not directly explain differences in Attack Index or Exposure Index, but it may help explain why organizations in similar environments do not always show similar levels of observed damage-related activity.

Taken together, these considerations suggest that industry should be understood as only one layer of explanation. It captures part of the external environment in which organizations operate, but it does not fully reflect the specific conditions of each organization.

Industry indicates tendencies, but risk is formed at the organizational level

An important implication of the results in this chapter is that industry is informative, but incomplete. Industry can help indicate broad tendencies in attack environment and provide a useful benchmark for relative comparison. However, the risk condition of an organization is formed more directly at the organizational level.

In practical terms, this means that organizations should not assume that their own risk condition is adequately represented by their industry average. Two organizations in the same industry may face very different attack pressure, exposure, and damage-related activity depending on their own environment and operations.

This point also strengthens the interpretation of the previous chapter. Industry-level comparisons remain useful because they reveal broad differences across sectors. But once the analysis moves from sector means to individual organizations, it becomes clear that within-industry variation is large enough that averages alone cannot represent the full picture.

For that reason, industry should be treated as a starting point for risk interpretation rather than as a final explanation. A fuller understanding of cyber risk requires looking at where each organization is positioned within the broader distribution of its sector.

The next chapter builds on this point by translating the analytical findings into practical principles for cyber risk management.

6

Principles of cyber risk management revealed by data

This chapter translates the analytical findings into practical principles for cyber risk management and uses a simple analogy to make the underlying logic easier to understand. These principles show that cyber risk is better understood as an interaction among Attack Pressure, Exposure, and apparent damage constraint.

Principles of cyber risk management revealed by data

Cyber risk management is not simply about facing fewer attacks. It is about reducing the likelihood that attacks succeed and limiting the extent to which harmful activity persists when they do.

The earlier analysis showed three broad points. First, Attack Pressure had the clearest overall relationship with observed Damage. Second, Exposure became more meaningful when organizations were already operating under harsher attack conditions. Third, even when both factors were considered together, meaningful variation in observed Damage still remained.

Taken together, these findings suggest that cyber risk should not be interpreted through isolated indicators, but understood as a structured interaction among the attack environment an organization faces, the exposure it has, and the organizational capability to constrain harmful activity in practice. The principles below summarize the practical meaning of that structure. They also provide a more interpretable way to understand cyber risk by clarifying why similar organizations may experience different outcomes, and why cyber risk management cannot rely on isolated indicators alone.

- **Principle 1: Cyber risk should not be interpreted through a single metric alone**

  One of the clearest findings in this study is that no single metric provides a sufficient view of cyber risk. Attack Pressure showed the strongest overall relationship with observed Damage, making it the most informative single signal in the dataset. However, even within similar Attack Pressure conditions, meaningful variation in Damage Months remained across organizations.

This means that Attack Pressure is highly informative, but not sufficient on its own. Exposure also matters, and the remaining variation suggests that additional factors influence how far harmful activity persists in practice. Cyber risk is, therefore, better understood through multiple interacting conditions rather than through a single score.

This matters for practical decision-making because isolated signals may be informative, but they are difficult to interpret and act on when viewed alone. A more useful interpretation of cyber risk comes from understanding how multiple conditions interact, rather than relying on any one metric in isolation.

- **Principle 2: The combination of Attack Pressure and Exposure is more informative than either factor alone**

  The analysis showed that Exposure had only a weak direct relationship with observed Damage when viewed on its own. However, much clearer differences appeared when Attack Pressure and Exposure were considered together.

  This was especially visible under high-attack conditions, where organizations with lower Exposure showed materially lower Damage Months than those with higher Exposure. In practical terms, this means that the same level of Exposure does not carry the same meaning in every environment. Exposure becomes more important when Attack Pressure is already high, and Attack Pressure becomes more actionable when interpreted together with Exposure.

  More broadly, this shows that cyber risk cannot be understood apart from context. The same exposure condition may have a very different practical meaning depending on the surrounding attack environment. What matters, therefore, is not exposure or pressure in isolation, but the way their interaction shapes practical risk.

- **Principle 3: Risk reduction requires both exposure reduction and damage constraint**

  A key implication of the findings is that organizations cannot manage cyber risk simply by trying to reduce the external Attack Pressure they face. In practice, the surrounding attack environment is often only partly controllable. The findings suggest that differences in Exposure and in the ability to constrain harmful activity play a central role in explaining why organizations experience different levels of observed Damage even under similar Attack Pressure conditions. This means that cyber risk reduction depends on two complementary efforts.

The first is to reduce the conditions that make attack success and initial compromise more likely, such as vulnerabilities, misconfigurations, and unnecessary exposure. The second is to strengthen the ability to detect, investigate, and contain harmful activity before it develops into more persistent harmful activity and, ultimately, observed damage.

In this sense, damage constraint is not separate from response capability; it is the observable effect of being able to detect, investigate, and contain harmful activity before it persists and leads to greater harm.

These three principles can also be understood through a simple driving analogy. Imagine that an organization is a person in a car driving through a dangerous environment. Attack Pressure corresponds to the severity of the external driving conditions: heavy rain, icy roads, poor visibility, or dense traffic. Exposure corresponds to weaknesses in the vehicle itself: worn tires, faulty brakes, or other factors that make it easier for danger to turn into an accident. Detection & Response Capability corresponds to the ability to recognize danger early, respond quickly, and maintain control before it worsens.

The first principle is that safety cannot be understood through only one factor. The risk of a vehicular accident is shaped by the interaction of road conditions, the vehicle's condition, and the ability to maintain control. Cyber risk works the same way—it reflects the interaction of multiple factors, not Attack Pressure alone.

The second principle is that the same weakness does not always have the same consequence in every environment: Worn tires may matter much more on an icy road than on a clear and dry one. Similarly, Exposure becomes more important when Attack Pressure is already high. The combination of Attack Pressure and Exposure is more informative than either factor alone.

The third principle is that managing risk requires both preparation and response: Safe driving depends not only on reducing weaknesses through maintenance, but also on recognizing hazards early and reacting effectively when danger appears. Similarly, cyber risk management requires both reducing exposure in advance and constraining harmful activity before it develops into more persistent damage.

Cyber risk is best understood not as the result of one factor, but as the outcome of interaction among the external attack environment, organizational exposure, and the extent to which harmful activity appears to be constrained in practice.

These three principles suggest that cyber risk management is not simply about experiencing fewer attacks but equally about reducing the likelihood that attacks succeed and limiting the extent to which harmful activity persists when they do. For practical decision-making, the same structure can be used not only to assess risk, but also to clarify whether improvement efforts should focus primarily on reducing exposure, strengthening response capability, or both.

The next chapter builds on this logic by introducing a Cyber Risk Positioning Map, a practical framework for understanding where an organization stands and what kind of improvement matters most.

7

Cyber Risk Positioning Map

The previous chapters showed that observed Damage is associated with both Attack Pressure and Exposure, and that meaningful differences remain even among organizations operating under broadly similar levels of those conditions. This matters because the surrounding risk environment alone does not fully explain why some organizations experience more persistent damage-related activity than others. To make those differences easier to interpret in practical terms, this chapter introduces a Cyber Risk Positioning Map.

The purpose of this map is not to predict future incidents. Rather, it provides a practical way to assess cyber risk from two perspectives at the same time: the severity of the broader risk environment an organization faces, and the extent to which harmful activity appears to be constrained within that environment. In that sense, the map is intended as a framework for interpretation and prioritization. It helps show not only where risk is high, but also where observed outcomes appear better or worse than the surrounding environment alone would suggest.

Framework design

The Cyber Risk Positioning Map uses two axes. The horizontal axis represents the CRI, and the vertical axis represents a Detection & Response Capability Score.

The CRI is used here as a practical summary indicator of the broader risk environment. In CREM, the CRI integrates multiple elements, including Attack Index and Exposure Index. In the earlier chapters of this study, Attack Pressure, Exposure, and Damage were examined separately to clarify their observed relationships. In this chapter, by contrast, the CRI is used as a broader summary measure for positioning organizations in terms of overall risk environment.

The vertical axis is designed to show how effectively harmful activity appears to be constrained relative to the Attack Pressure an organization faces. To make this visible in a simple and comparable way, this study introduces a supplementary Detection & Response Capability Score defined as follows:

$$\textbf{Detection \& Response Capability Score} = \frac{\textbf{Attack Index}}{\textbf{Damage Months} + 1}$$

The logic of this score is intentionally simple. If an organization faces relatively high Attack Pressure but shows fewer Damage Months, harmful activity may be constrained more effectively in practice. Conversely, if damage-related activity remains relatively high even under lower or moderate Attack Pressure, harmful activity may be constrained less effectively relative to the observed environment. The "+1" in the denominator is included to avoid division by zero when Damage Months is zero.

This score is not intended as a direct measure of security maturity or operational quality. More specifically, it should be interpreted as a comparative proxy for apparent damage constraint under observed attack conditions, not as a direct measurement of operational capability. Its purpose is to make one practical distinction more visible: Organizations facing similar levels of overall risk do not always appear equally effective at limiting persistent damage-related activity. That distinction cannot be understood from the CRI alone.

In the figure, bubble size represents the number of organizations included in each group, and color represents mean Damage Months. Dashed lines indicate the mean values of the CRI and Detection & Response Capability Score and divide the figure into four quadrants.

Quadrant	Meaning
Secure position	A relatively calm risk environment with comparatively stronger detection and response capability
Resilient target	A more severe risk environment, but with comparatively stronger detection and response capability
Latent risk	A less severe current risk environment, but with comparatively weaker detection and response capability
Critical risk	A more severe risk environment with comparatively weaker detection and response capability

Table 4. Interpretation of the Cyber Risk Positioning Map quadrants

Taken together, these two axes provide a practical way to understand cyber risk not only through the severity of the environment an organization faces, but also through the extent to which harmful activity appears to be constrained within that environment. This is the central value of the framework.

The Industry Cyber Risk Positioning Map

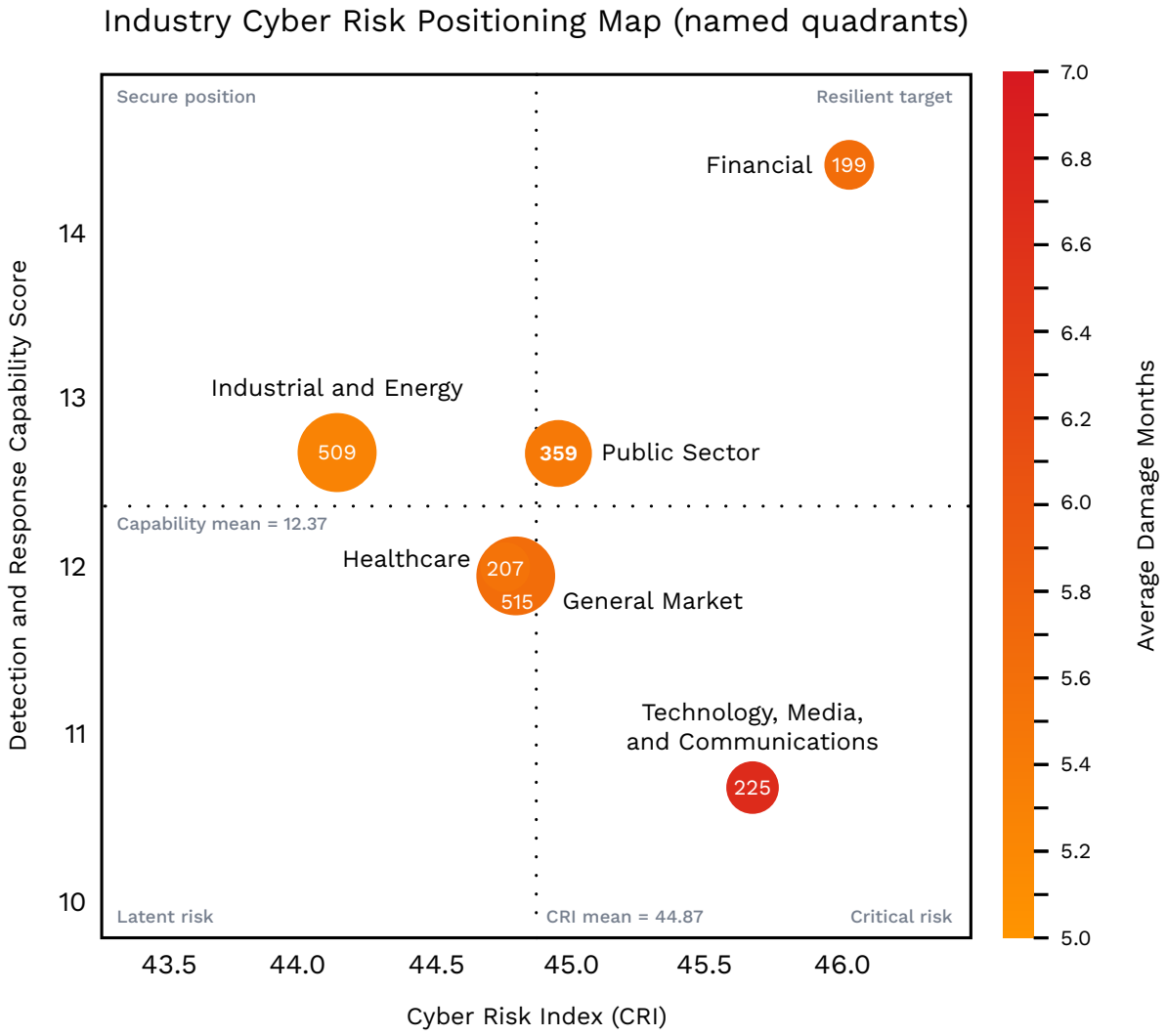

Figure 8. The Industry Cyber Risk Positioning Map
Note: The numbers in each circle specify the sample size for each industry group.

Figure 8 applies the Cyber Risk Positioning Map to the six industry groups. It shows that industries differ not only in the severity of the risk environment they face, but also in how effectively harmful activity appears to be constrained within that environment. This matters because industries positioned at similar levels of overall risk do not necessarily show similar damage-related outcomes.

The clearest example is the comparison between the Financial and the Technology, Media, and Communications groups. Both groups appear in relatively high-CRI positions, indicating broadly severe risk environments. However, Technology, Media, and Communications appears lower on the vertical axis than Financial, indicating a comparatively lower Detection & Response Capability Score. This is consistent with

the earlier finding that the two groups faced similarly high Attack Pressure, while Technology, Media, and Communications showed higher Damage Months.

This contrast illustrates the practical value of the framework. The CRI helps show how severe the surrounding risk environment is, but it does not by itself explain why outcomes differ under broadly similar conditions. The vertical axis makes that difference easier to interpret by showing whether harmful activity appears to be more or less constrained relative to the observed environment.

The other industry groups reinforce the same point. The Public Sector group appears close to the center of the map, reflecting a position near the overall average on both axes. The Healthcare and Industrial and Energy groups appear in relatively lower-CRI areas, while the General Market group occupies a somewhat higher CRI but more moderate vertical position. Together, these placements show that industry differences are visible not only in overall risk environment, but also in how observed outcomes compare within that environment.

These positions should not be interpreted as absolute judgments about overall security effectiveness. Rather, they provide a comparative view of how observed damage-related activity relates to overall risk environment across industry groups. In that sense, the Industry Cyber Risk Positioning Map is useful not because it gives a final answer, but because it makes differences in relative position easier to see and interpret.

How organizations can use the framework

The practical value of the Cyber Risk Positioning Map lies in helping organizations understand their current position more clearly. The first step is to identify where the organization sits on the map. The second is to interpret what that position implies about its cyber risk.

Organizations positioned toward the right side of the map are operating in a more severe risk environment and should focus more closely on reducing exposure and understanding which external conditions are driving that position. Organizations positioned lower on the map should examine whether harmful activity is being constrained effectively relative to the attack pressure they face. Organizations in the lower-right area should treat both issues as priorities.

Seen in this way, the map is not only a benchmarking tool but also a prioritization tool. It helps organizations move from a general sense of cyber risk to a more practical question: What kind of improvement is most needed now? For some organizations, the

priority may be reducing exposure or improving the ability to detect, investigate, and contain harmful activity. For others, both may need to be addressed simultaneously.

The framework is also useful over time. By reassessing position as telemetry changes, organizations can see whether they are moving toward a more favorable risk structure or whether the same underlying issues remain. In this sense, the Cyber Risk Positioning Map is useful not only for interpretation, but also for ongoing review and prioritization.

8

Conclusion

Closing perspective

This study showed that cyber damage is not best understood through any single indicator alone. Attack Pressure provided the clearest overall signal, but it did not fully explain why similar organizations still showed different levels of persistent damage-related activity. Exposure also did not carry the same meaning in every environment. Its importance became clearer under harsher attack conditions, especially when considered together with Attack Pressure rather than in isolation.

Seen in this way, cyber risk is better understood not as a collection of isolated measures, but as a structured relationship among the environment an organization faces, the exposure it has, and the extent to which harmful activity appears to be constrained in practice. In other words, differences in observed Damage are not explained by attack intensity alone, but by how Attack Pressure, Exposure, and damage constraint interact under real-world conditions.

The value of this perspective is practical as well as analytical. It shifts the discussion away from isolated scores and toward a more interpretable view of why outcomes differ. That makes cyber risk easier not only to assess, but also to explain in clear and practical terms.

For security leaders and other decision-makers, this matters because risk often has to be communicated beyond the security team, to operational stakeholders, business leadership, and others involved in prioritization and action. This is especially important because, across different organizational and industry contexts, similar patterns of risk may still carry different practical meanings and call for different priorities in response.

In that sense, the most important shift is not simply to ask how much risk an organization faces, but to understand how the different elements of that risk interact. This helps organizations assess cyber risk more clearly, prioritize improvement more effectively, and manage risk with greater confidence. It also reinforces a broader lesson from this research and the earlier work on exposure reduction and response capability on which it builds: these are not separate concerns, but complementary parts of a more interpretable and actionable approach to managing cyber risk.

Call to action

To act on cyber risk more effectively, organizations should move beyond interpreting risk through isolated indicators alone. The CRI provides a useful summary view of the overall risk environment, but the next step is to interpret how Attack Pressure, Exposure, and damage constraint interact within that environment—and use that structure to guide action.

In practice, this means reducing the conditions that make compromise more likely and strengthening the conditions that limit post-compromise harm. Reducing vulnerabilities, misconfigurations, and unnecessary exposure can lower the conditions that make successful compromise more likely. Strengthening the ability to detect, investigate, and contain harmful activity can help prevent successful intrusions from developing into more persistent damage-related activity.

A more structured interpretation of cyber risk should shape more than technical analysis. It should also support clearer prioritization, stronger alignment, and better-informed decisions across security, operational, and leadership stakeholders.

Organizations should begin with three practical actions:

- Identify what is driving the CRI in their environment.
- Identify which exposure conditions most need to be reduced.
- Determine where harmful activity is not being constrained effectively enough.

By using CREM for visibility into exposure conditions and XDR for visibility into attack progression and containment outcomes, organizations can use TrendAI Vision One™ capabilities to turn cyber risk into clearer management priorities.

Limitations

Several limitations should be kept in mind when interpreting these findings. First, the analysis is based on observed telemetry data from TrendAI Vision One™ and is limited to the organizations included in this analytical population. The results, therefore, provide an empirical view of the organizations studied, but should not be interpreted as directly representative of all organizations or all operating environments.

Second, the analysis is observational and focuses on association rather than causation. While the findings show how Attack Pressure, Exposure, and observed damage-related activity were related within the dataset, they do not establish that one factor directly causes another.

Third, Attack Index and Damage Months are both derived from XDR-observed attack activity, although they represent different stages and analytical purposes. Because of this, the observed relationship between Attack Pressure and Damage may be strengthened in part by their shared telemetry foundation. This does not remove the practical value of the finding, but it does mean that the relationship should be interpreted as an empirical association within the observed telemetry framework rather than as a fully independent comparison between unrelated measures.

Fourth, Damage Months is a proxy indicator based on observed later-stage attack behavior. It is useful for comparing the persistence of damage-related activity, but it does not directly measure financial loss, operational disruption, or broader business impact.

Fifth, the Detection & Response Capability Score introduced in Chapter 7 is a comparative proxy indicator, not a direct measure of security maturity or operational quality. Its purpose is to help interpret how harmful activity appears to be constrained relative to Attack Pressure, not to provide a complete measure of defensive capability.

Taken together, these limitations do not reduce the practical value of the study, but they do define its scope. The findings are best understood as a structured, data-driven, and empirically bounded view of cyber risk within the observed population, rather than as a complete or universally generalizable model of cyber damage.

Future work

This study focused on organization-level relationships among Attack Pressure, Exposure, and observed damage-related activity. However, a more detailed understanding of cyber risk structure would benefit from further analysis across additional perspectives.

One important direction is to examine how these relationships differ by attack type or tactic. The way Attack Pressure and Exposure relate to Damage may not be identical across ransomware, data theft, disruptive activity, or other forms of attack behavior.

A second direction is to examine organizational and industry context in greater detail. Industry was useful for understanding broad differences in risk environment, but substantial variation remained within the same industry. Future analysis may, therefore, benefit from looking more closely at factors such as region, digital footprint, infrastructure model, or organizational complexity.

A third direction is to refine how damage constraint is interpreted in practice. The comparative framework introduced in this study provides one practical view, but future work may strengthen that interpretation further by incorporating more direct operational indicators of detection, investigation, response, and containment where available.

A related direction is to strengthen how cyber risk can be interpreted and communicated in practice by integrating more direct operational indicators into this comparative framework. This may help make the structure of cyber risk more actionable not only for analysts, but also for those responsible for prioritization, coordination, and decision-making.

Through such extensions, future research may provide a clearer and more actionable view of how cyber risk is formed and how it can be managed more effectively.

Want more insights like this?

trendmicro.com/SECNEWS

TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk.

Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data.

AI Fearlessly.

Learn more: **trendaisecurity.com**