X-Analytics Board Insights:
Cyber and AI Risk
Empowering Boards with Advanced Cyber & AI Risk Intelligence

X-ANALYTICS

Cyber and AI risks shouldn't be buried in Item 1A risk factors - they are operational, strategic, and financial threats that demand active board oversight. Yet boards are still being asked to govern these risks with compliance checklists, heatmaps, and vague maturity models that fail to deliver business-relevant insight.

Selected by the NACD

These threats aren't waiting for audit to catch up...

- **Ransomware** disrupts core operations.
- **AI models** fail silently, introducing bias, error, or regulatory exposure.
- In both cases, **financial stakes are rising**.

Effective oversight requires more than red/yellow/green charts. It requires **financial exposure, scenario modeling, and governance-ready insight** - delivered in language that empowers the board.

X-Analytics Board Insights: Cyber and AI Risk transforms fragmented threat data into financially contextualized intelligence. Trusted by boards, insurers, and regulators alike, X-Analytics empowers directors to ask better questions, make smarter decisions, and meet emerging accountability standards head-on.

Navigate the complex world of cyber and AI risk with X-Analytics

X-Analytics advanced business analysis delivers **actionable insights** and predictive analytics. With these, business leaders can have the confidence knowing investments are focused on those areas that bring tangible business benefit.

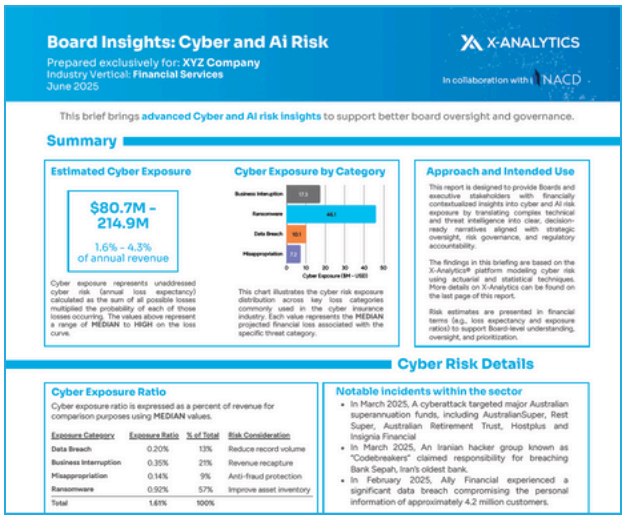
Cyber audits and assessments are nice, but X-Analytics **elevates** cyber and AI risk insights driving greater business context and value.

Board-ready Cyber Risk Insights

Selected by the National Association of Corporate Directors (NACD), X-Analytics delivers Board-ready cyber risk Insights.

Fortune 500 Tested

X-Analytics is proven to deliver value in some of the largest public corporations in the world.


Board Insights: Cyber and Ai Risk

Prepared exclusively for: XYZ Company
Industry Vertical: Financial Services
June 2025

X-ANALYTICS

In collaboration with NACD

This brief brings advanced Cyber and AI risk insights to support better board oversight and governance.

Summary

Estimated Cyber Exposure

$80.7M - 214.9M

1.6% - 4.3% of annual revenue

Cyber exposure represents unaddressed cyber risk (annual loss expectancy) calculated as the sum of all possible losses multiplied the probability of each of those losses occurring. The values above represent a range of MEDIAN to HIGH on the loss curve.

Cyber Exposure by Category

Business Interruption
Ransomware
Data Breach
Misappropriation

This chart illustrates the cyber risk exposure distribution across key loss categories commonly used in the cyber insurance industry. Each value represents the MEDIAN projected financial loss associated with the specific threat category.

Approach and Intended Use

This report is designed to provide Boards and executive stakeholders with financially contextualized insights into cyber and AI risk exposure by translating complex technical and threat intelligence into clear, decision-ready narratives aligned with strategic oversight, risk governance, and regulatory accountability.

The findings in this briefing are based on the X-Analytics® platform modeling cyber risk using actuarial and statistical techniques. More details on X-Analytics can be found on the last page of this report.

Risk estimates are presented in financial terms (e.g., loss expectancy and exposure ratios) to support Board-level understanding, oversight, and prioritization.

Cyber Risk Details

Cyber Exposure Ratio

Cyber exposure ratio is expressed as a percent of revenue for comparison purposes using MEDIAN values.

Exposure Category	Exposure Ratio	% of Total	Risk Consideration
Data Breach	0.20%	13%	Reduce record volume
Business Interruption	0.35%	21%	Revenue recapture
Misappropriation	0.14%	9%	Anti-fraud protection
Ransomware	0.92%	57%	Improve asset inventory
Total	1.61%	100%	

Notable incidents within the sector

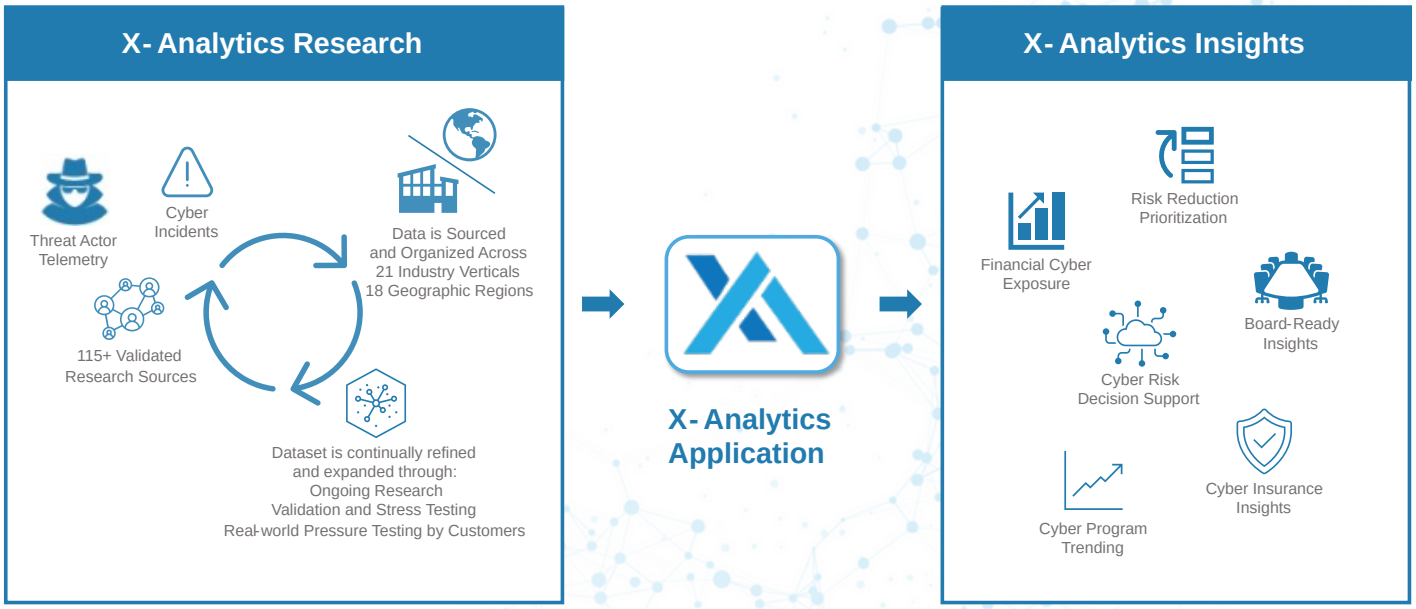
- In March 2025, A cyberattack targeted major Australian superannuation funds, including AustralianSuper, Rest Super, Australian Retirement Trust, Hostplus and Insignia Financial
- In March 2025, An Iranian hacker group known as "Codebreakers" claimed responsibility for breaching Bank Sepah, Iran's oldest bank.
- In February 2025, Ally Financial experienced a significant data breach compromising the personal information of approximately 4.2 million customers.

X-ANALYTICS

X-Analytics delivers expanded value for cyber and AI governance

The X-Analytics data behind the report

X-Analytics draws on a patented methodology, which integrates industry-aligned threat context, control effectiveness measures, and enterprise-specific attributes. These insights are trusted and actively used by leading cyber insurance providers to model their real-world loss scenarios.



Cyber and AI Risk in the Language of Business

A core strength of X-Analytics is its ability to bring a business lens to cyber and AI risk. Understand the potential financial impact of cyber incidents, enabling you to make data-driven decisions about risk mitigation and insurance coverage.

Actionable Insights for Ongoing Improvement

Common cyber assessments provide a framework for technical improvement; X-Analytics delivers actionable business insights. This helps organizations understand the effectiveness of their cybersecurity measures and identify areas for ongoing improvement.

Strategic Decision-Making

X-Analytics equips organizations with the business insights needed to make informed strategic decisions regarding cybersecurity and AI investments and resource allocation. This strategic approach ensures that investments in cybersecurity deliver the greatest possible business value.

Ready to lead on cyber and AI risk governance?

Contact us today to learn more about how X-Analytics can help boards make informed decisions and safeguard your business.

Visit www.x-analytics.com to learn more.

X-Analytics® is a registered trademark of Secure Systems Innovation Corporation.
All rights reserved.

www.x-analytics.com