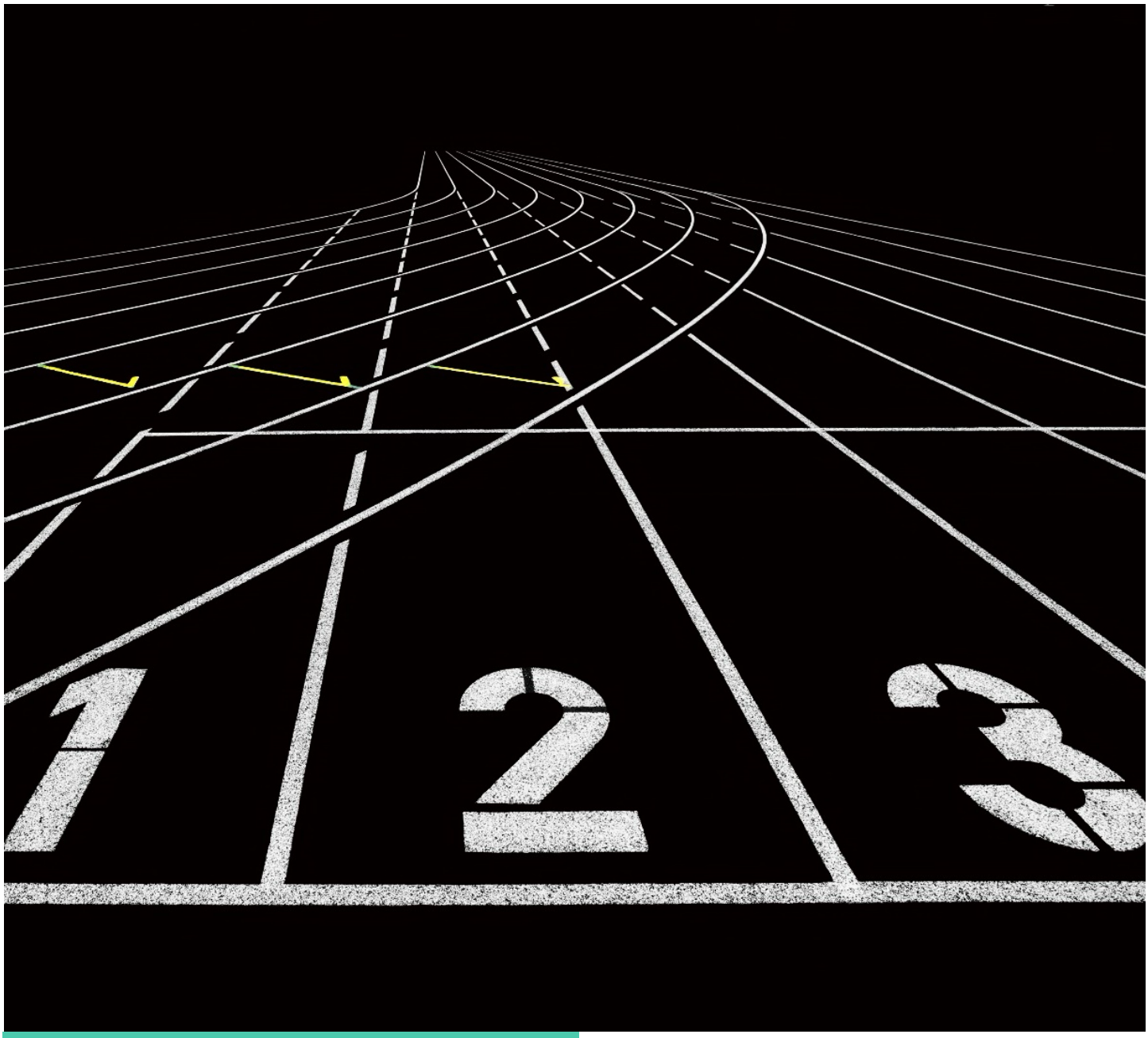
| BOARD OF DIRECTORS MUST-READ |

REVOLUTIONIZING BOARD OVERSIGHT IN CYBER RISK

ARXNIMBUS.COM | ERDADICATE CYBER RISK info@arxnimbus.com



CYBER RISK MEETS FINANCIAL CLARITY.

Cyber risk oversight is no longer just about technical defenses—it's about financial resilience and strategic governance. With threat landscapes constantly evolving, boards face mounting pressure to move beyond compliance checklists and embrace data-driven decision-making.

Cue the ArxNimus actuarial-based risk quantification platform, delivering clear, board-ready insights and empowering directors to collaborate with leadership to make confident, well-informed governance decisions.

EXECUTIVE SUMMARY

In today's digital business environment, boards face unprecedented challenges in fulfilling their oversight responsibilities for cybersecurity and digital risk. Traditional approaches to risk reporting and measurement increasingly fail to provide boards with the insights needed for effective governance and strategic decision-making.

This position paper examines how ArxNimbus transforms board oversight through actuarial-based risk quantification, enabling directors to make informed decisions about cyber risk management and strategic investments. Our approach provides the clarity, structure, and actionable insights necessary for boards to fulfill their fiduciary responsibilities effectively.

Let's explore how the ArxNimbus platform revolutionizes cyber risk oversight at the board level.

THE BOARD'S CHALLENGE: UNDERSTANDING AND MANAGING CYBER RISK

Recent high-profile breaches highlight a critical gap in how organizations approach cyber risk management at the board level. The Change Healthcare breach, resulting in billions in losses with only $100 million in insurance coverage, demonstrates how traditional risk assessment methods can dramatically underestimate actual exposure. This gap between perceived and actual risk creates significant governance challenges for boards.

.

Current Board-Level Challenges:

- **Limited Risk Visibility:** Traditional reporting methods often provide boards with technical metrics that don't translate into meaningful business insights. When presented with statistics about blocked attacks or patched vulnerabilities, directors cannot effectively evaluate their organization's risk exposure or the adequacy of their security investments.

- **Investment Uncertainty:** Without clear financial metrics for cyber risk exposure, boards struggle to make informed decisions about security investments and resource allocation. This uncertainty often leads to either under-investment in critical areas or inefficient allocation of security resources.

- **Strategic Alignment:** Traditional approaches frequently fail to connect security initiatives with business strategy and objectives. This disconnect makes it difficult for boards to ensure that security investments support and enable business growth rather than merely addressing technical compliance requirements.

- **Governance Effectiveness:** Many boards lack the quantitative insights needed to fulfill their governance responsibilities effectively. This gap exposes both the organization and individual directors to potential liability when significant security incidents occur.

The case study below highlights this discrepancy in action. A global bio-pharma company initially estimated its personally identifiable information (PII) breach risk at $25 million using internal assessments. However, a data-driven analysis leveraging actuarial cyber risk quantification revealed a vastly different reality: the true financial exposure exceeded $190 million—a nearly **87% underestimation**. This stark contrast underscores the critical need for boards to adopt more precise, quantitative approaches to cyber risk assessment.

Comparison with Legacy Methods

Case Study: $170bn Global Bio-Pharma Customer

Before / Status Quo / Opinion-Driven	Thrivaca™ Data-Driven Results
PII BREACH RISK Customer developed an "estimation" of PII Worst-Case Scenario with internal expert opinion inputs	**PII BREACH RISK** ▪ Over 200mm non-duplicate HIPAA records in customer's possession ▪ Thrivaca provided an attacker-value analysis of target value based on current/recent dark-web transactions ▪ Hardcopy notification costs of $62mm ▪ Scaled historical comparables showed equity losses of $88mm ➔ *Four-day trading period* ▪ Associated Incident Response costs of $42mm ➔ *Fines/Fees/PR/Litigation/Post-Remediation*
ESTIMATION: $25MM	**RESULT: $192MM**

△ = 86.9%

IN MANAGING YOUR DIGITAL RISKS—WHICH DO YOU PREFER?

ArxNimbus

HOW THE ARXNIMBUS SOLUTION ENABLES EFFECTIVE BOARD OVERSIGHT

ArxNimbus transforms how boards understand and oversee cyber risk through our actuarial-based approach to risk quantification. Our solution provides directors with clear, actionable insights that enable effective governance and strategic decision-making.

Quantitative Risk Understanding

Our platform translates complex technical risks into clear financial metrics that board members can understand and act upon. This includes:

- **Financial Exposure Quantification:** Precise calculation of potential losses from various types of cyber incidents, enabling comparison with other business risks.

- **Investment Return Analysis:** Clear measurement of how security investments reduce risk exposure, supporting informed decision-making about resource allocation.

- **Risk Transfer Evaluation:** Detailed analysis of insurance coverage adequacy and self-insured risk exposure, enabling better risk transfer strategies.

Strategic Alignment

ArxNimbus enables boards to ensure alignment between security investments and business objectives through:

- **Business Impact Analysis:** Clear connection between security initiatives and business outcomes, ensuring security investments support strategic goals.

- **Comparative Benchmarking:** Industry-specific comparisons that help boards understand their organization's security posture relative to peers.

- **Strategic Planning Support:** Data-driven insights that enable better integration of security considerations into strategic planning and digital transformation initiatives.

Governance Advancement

Through its integration of actuarial-based risk quantification including AI-specific framework requirements, our solution strengthens board governance capabilities through:

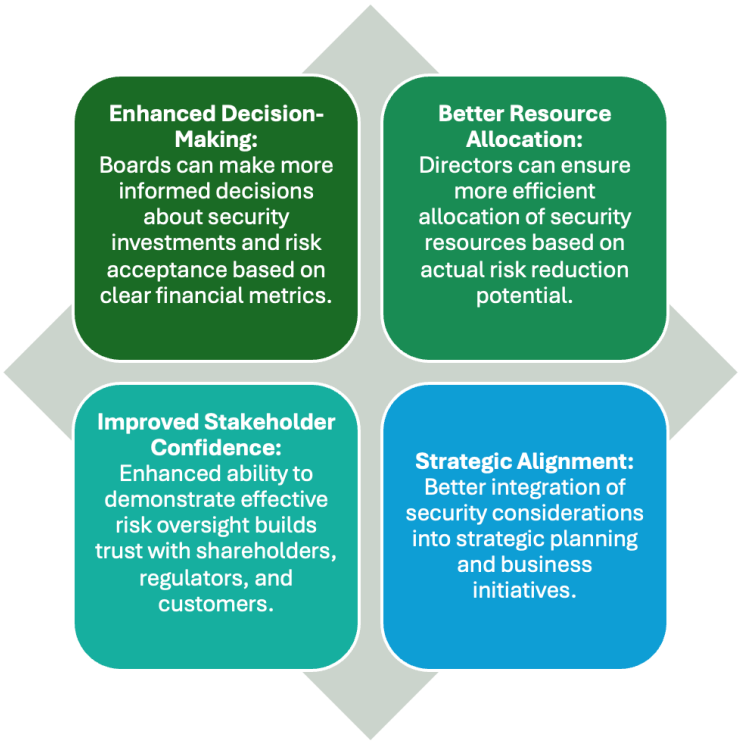
- **Comprehensive Oversight:** Clear visibility into overall risk exposure and management effectiveness, supporting better governance decisions.

- **Regulatory Compliance:** Alignment with emerging regulatory requirements for board oversight of cybersecurity risk.

- **Stakeholder Communication:** Enhanced ability to demonstrate effective risk oversight to shareholders, regulators, and other stakeholders.

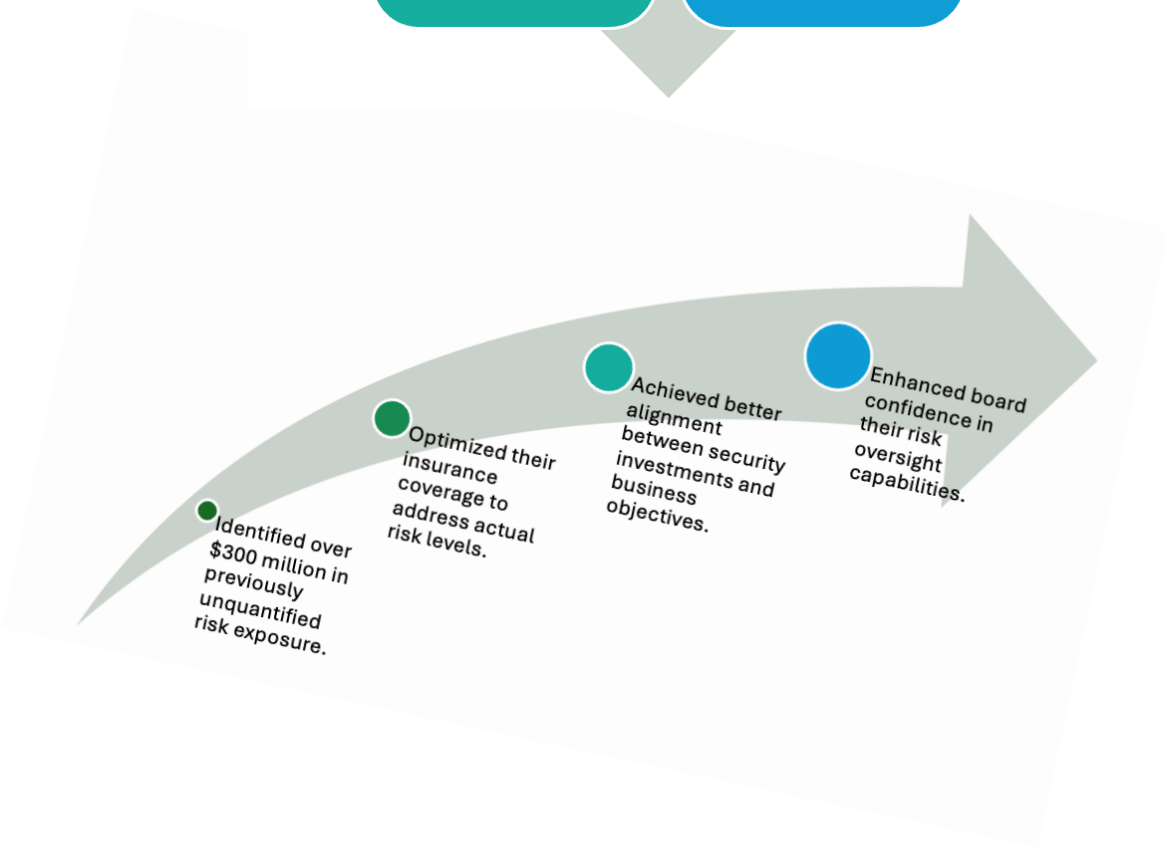
TRANSFORMATIONAL IMPACT

Organizations implementing ArxNimbus typically experience several significant improvements in board effectiveness:



REAL-WORLD RESULTS

Our experience with Fortune 500 companies demonstrates the transformative impact of our approach. For example, a global financial services organization using ArxNimbus:



CONCLUSION: THE PATH FORWARD

In today's complex risk environment, boards can no longer rely on traditional approaches to cyber risk oversight. The ArxNimbus solution provides the comprehensive, data-driven approach needed for effective governance in the digital age.

By transforming how boards understand and oversee cyber risk, ArxNimbus enables directors to fulfill their governance responsibilities more effectively while ensuring better protection of shareholder value. Our actuarial-based approach provides the clear metrics and actionable insights needed for strategic decision-making at the board level.

The time has come for boards to evolve beyond traditional risk oversight approaches. With ArxNimbus, directors can achieve the comprehensive risk visibility and control needed to ensure effective governance in today's digital business environment.

.

ABOUT THE AUTHORS

R. David Moon, CEO and co-founder of ArxNimbus, is a quant-focused cybersecurity risk specialist, Fortune 500 CIO, CISO, Big Four consulting partner, CISSP, software industry product manager and senior officer.

A four-year US Air Force veteran with Secret clearance, David is an expert information security and executive-level technology professional with a 20+ year portfolio of some of the most ground-breaking and high-value project results in information security, technology, privacy, asset management, IT risk management and infrastructure.

For more than a decade he has been privileged to serve and consult to some of the world's most respected organizations in the United States, Latin America, and Europe. His writing includes examining the measurable value of technology-based capability and its role in risk mitigation in the 2011 book "Webify" (https://www.amazon.com/Webify-Interconnections-Strategy-Capability-Volatility-ebook/dp/B006RX4PXM). He has served on the board of a public investment trust and as a member of the senior executive committee of a $5bn Nasdaq company.

Andrew Patterson, COO of ArxNimbus, leads the delivery and optimization of advanced cyber and AI risk management solutions. His distinctive background bridges public service and private sector expertise in global risk management.

Prior to joining ArxNimbus, Andrew held several high-level positions in government, including Deputy Chief of Staff and Global Risk Advisor at the U.S. Department of Energy and liaison to the National Security Council. In these roles, he shaped critical risk management strategies at the highest levels of government decision-making.

Andrew's private sector experience encompasses strategic positions with PwC's Research and Insights team, where he analyzed emerging global risks and trends. His background also includes significant work with leading hedge funds and commodity traders, helping these organizations anticipate and navigate complex operational and portfolio risks.

In his decades of risk management experience, Andrew has pioneered a unique methodology that integrates advanced analytics with hands-on implementation expertise, empowering organizations to proactively identify and address emerging cyber threats.

ABOUT ARXNIMBUS | *CYBERSECURITY FOR BUSINESS*

ArxNimbus brings visibility to every organization's cybersecurity program, radically advancing how businesses understand and optimize for real resilience. Our passion is illuminating actionable intel of cybersecurity risk to enterprises, investors, advisors, and insurers worldwide. Our Thrivaca™ technology, commissioned by US Strategic Command and designed by leading economists and actuaries, uses fact-based, mathematically modeled analyses of the threat landscape. ArxNimbus applies this Thrivaca platform to cross-correlate the effects of Threats, Vulnerabilities, and Capabilities on cybersecurity risk root causes. This foundational technology now powers the **only NIST-based AIA risk management platform** for today's AI initiatives.

Contact: info@arxnimbus.com **| 888-422-6584|** ArxNimbus.com

Follow us for the latest cyber risk insights, trends, and Risk Call Events: