AN ARXNIMBUS POSITION PAPER

BEYOND DASHBOARDS

Why CTEM must become Financial Exposure Intelligence

>25% **of EBITDA.**

The unquantified cyber exposure most organizations carry — invisible on every dashboard.

READ THE PAPER

ArxNimbus
Secure the business.

#ProtectYourEBITDA · It's not magic. It's math.

ArxNimbus.com

AN ARXNIMBUS POSITION PAPER · ENTERPRISE / BOARD EDITION

Beyond Dashboards: Why CTEM Must Become Financial Exposure Intelligence

By R. David Moon, CEO & Co-Founder, and Andrew Patterson, COO · ArxNimbus

The thesis in one line. Continuous Threat Exposure Management is the right direction. But visibility was never the destination. The destination is financial exposure leaders can explain, defend, and act on.

1 CTEM is a real step forward. Most people are still underselling it.

For years, cybersecurity ran on a calendar: an annual assessment, a static report, a number already stale by the time the board saw it. Continuous Threat Exposure Management broke that habit. It treats exposure the way the business actually behaves — continuously. New assets appear. Software dependencies shift. AI tools get adopted. Controls degrade. Vendors introduce risk no one approved.

A once-a-year snapshot cannot keep up with that pace, and CTEM is right to say so. Good CTEM continuously monitors exposure, unifies signals across a sprawling tool stack, prioritizes by business impact, and tracks current exposure against projected exposure after controls.

That last capability is the one that matters most. And it is the one most CTEM programs never finish building.

$244B[1] spent on security globally. **76**[2] tools in the average enterprise. And boards still cannot get a defensible answer to the only question that matters.

2 "We have a dashboard" was never the problem CTEM set out to solve.

Cyber dashboards have become the common operating picture for most organizations. They show alerts, findings, control activity, vulnerability counts, severity scores, status indicators. That information has value. But it quietly creates a false sense of decision support.

A red indicator tells a leader something needs attention. It does not tell them how much financial exposure that issue creates, whether it matters more than the other forty red indicators, what to fund first, or how much exposure a fix will actually remove.

This is the gap leaders feel the moment cyber risk reaches the boardroom. More than 90% of directors now regard cyber risk as a direct threat to shareholder value — and more than 90% lack confidence in the value of their cybersecurity investments.[3] They see the threat clearly. They cannot grade the response.

[1] Gartner — worldwide information security spending forecast; projected at $244B for 2026.
[2] Panaseer — survey of 1,200 security decision-makers; average enterprise operates 76 security tools.
[3] Gartner — 2026 Board of Directors Survey.

Security teams can describe activity. Boards need to understand exposure. CFOs need to understand financial impact. And a dashboard can prove that work is happening — it cannot prove that risk is going down in a way the CFO can put in a forecast.

3 Where CTEM stalls: visibility without a number.

CTEM improves visibility, prioritization, and operational focus. But if it stops there — if it never translates exposure into financial terms — it leaves leadership with a more sophisticated version of the same incomplete answer. The gap is precise:

What CTEM can tell you	What it leaves unpriced
✓ what changed	✕ how much it costs, in dollars
✓ where the exposure sits	✕ how much investment removes it
✓ how it is trending over time	

The board does not need to become fluent in another acronym. The CFO does not need another technical score. They need a defensible way to understand business exposure, in the same units they use for every other decision they make.

> ***"We patched a lot" is not the same as "we reduced exposure."***

That sentence is the whole problem. Activity is easy to report. Reduction is hard to prove. And without proof of reduction, every cyber budget conversation defaults to faith, fear, or last year's number plus ten percent.

And the exposure that goes unpriced is not marginal. ArxNimbus modeling across our 4,000+ company risk-profile library shows that enterprises routinely carry unquantified cyber exposure exceeding 25% of EBITDA — exposure no dashboard is built to surface.[4]

4 The missing layer: financial exposure intelligence.

Financial exposure intelligence is what connects cyber, software, AI, and control data to business and financial outcomes. It answers the questions leadership actually asks: How much exposure do we carry today? Where is it concentrated? Which exposures create the greatest potential financial impact? Which investments reduce exposure most efficiently? How does exposure change after we remediate? What does it mean for EBITDA, ROI, resilience, and how we think about risk transfer?

The shift is simple to state and hard to deliver:

- **Visibility** tells you what exists.

[4] ArxNimbus data foundation: 4,000+ company risk-profile library, 60,000+ cyber-incident loss database, 47,000+ threat-vulnerability pairings, 32 primary authoritative sources, 580+ industries; engine validated against documented loss events to within 7%.

- **Quantification** tells you what it means.
- **Financial exposure intelligence** tells you what to do next.

Done right, it produces two defensible numbers a board can govern against — built on actuarial models rather than heat maps and professional judgment:

Current financial exposure	Projected exposure after controls
what we carry today, in dollars	what changes when we invest

That is the difference between reporting and decision intelligence. A dashboard shows a high-risk finding. CTEM shows the finding is trending worse. Financial exposure intelligence shows what that trend costs and what action removes it.

And the payoff is measurable, not theoretical. Across the ArxNimbus client base, exposure reduction typically translates into a 1–3% average annual EBITDA improvement — on an engine validated against documented loss events to within 7%.

5 Why now — and why this gets bigger, not smaller.

Cyber risk no longer lives inside the security function. It intersects directly with operational resilience, AI governance, software supply chain risk, insurance, M&A, compliance, customer trust, and enterprise value. At the same time, executives are being asked to make faster decisions under more uncertainty — approving AI initiatives, defending budgets, reviewing coverage, answering regulators, and explaining posture to investors.

The old model of cyber reporting does not provide enough decision support for that environment. Leaders need to move from alerts, to exposure, to financial impact, to prioritized action, to *measurable reduction.*

And here is the part most organizations have not internalized yet: the same blind spot is now forming around AI. The fragmented-signals-no-financial-number pattern that produced a decade of cyber dashboards is repeating — faster — with AI systems being adopted ahead of the governance to measure them.

> **88%** of organizations now use AI in at least one part of the business. **8%** have a comprehensive framework to govern it.[5] **That 10× gap is the next exposure crisis — forming in plain sight, in exactly the pattern this paper just described.**

It is not hypothetical. Two-thirds of executives already believe their organization has suffered a data leak through unapproved AI tools.[6] The organizations that learn to quantify exposure now, in dollars, will be the ones able to govern AI risk when it matters. The ones still arguing over severity scores will not.

[5] AI adoption data per Aon; AI-governance-framework data per Economist Impact.
[6] Writer — State of Enterprise AI 2026.

6 What leaders should actually demand from exposure management.

As CTEM gains traction, the temptation is to treat it as another reporting category to check off. The better test is not *"Do we have CTEM?"* It is *"Can our exposure program answer the questions leadership actually needs answered?"*

- Can we quantify exposure in financial terms?
- Can we compare exposure across cyber, software, and AI risk on one scale?
- Can we prioritize remediation by business impact, not just severity?
- Can we model the projected effect of controls *before* we spend?
- Can we track exposure reduction *after* we invest?
- Can we explain all of it in terms the board and the CFO already use?

If the answer is no, the organization has more visibility — but not more clarity. Boards do not need more acronym fluency. They need exposure clarity. The acronym matters less than the answer.

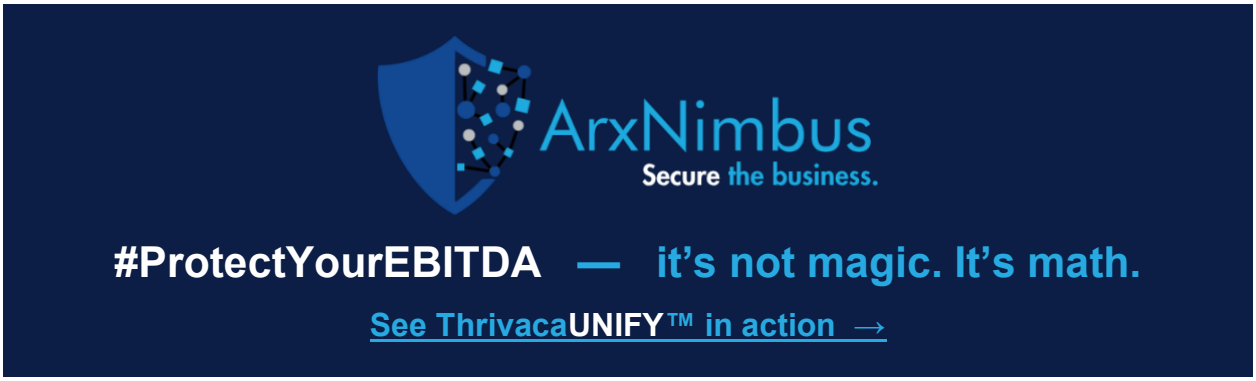
7 Where ArxNimbus fits.

This is the gap **ThrivacaUNIFY™** was built to close: the only actuarial CTEM platform that converts fragmented security telemetry into defensible financial exposure — built on a NIST-designed methodology, across infrastructure, software, and AI — and delivers it as two numbers a board can govern against, not another dashboard to interpret. Built on an actuarial engine validated with leaders across national security, academia, and industry, it brings insurer-grade rigor to the exact questions above. The same engine underwrites cyber exposure for 35% of the S&P 500.

Nine years of AI. Not nine months.

How much exposure do we carry? Where is it coming from? What reduces it? What does it mean to EBITDA and ROI?

That's the conversation modern exposure management should make possible.



About ArxNimbus

ArxNimbus was built on a simple idea: AI and actuarial modeling, together, are the most reliable way to measure exposure in financial terms. Since 2016, we have used AI to normalize fragmented security data and actuarial science to quantify its financial impact — producing a continuous, defensible system of record for enterprise exposure.

Built in collaboration with leaders across national security, academia, and industry — including MITRE, the University of Chicago, and the U.S. Department of Defense — the **Thrivaca**™ engine reflects how risk is actually modeled and validated in the real world. **ThrivacaUNIFY**™ applies that engine to continuously quantify enterprise exposure — bringing insurer-grade financial rigor to cybersecurity operations, prioritization, and executive decision-making.

About the authors

R. David Moon — Chief Executive Officer & Co-Founder

R. David Moon is a quant-focused cybersecurity risk specialist whose career spans Fortune 500 CIO and CISO roles, a Big Four consulting partnership, and senior software-industry leadership. A CISSP and four-year U.S. Air Force veteran with Secret clearance, he brings a 20-plus-year portfolio of high-value work across information security, privacy, IT risk management, asset management, and infrastructure — advising some of the world's most respected organizations across the United States, Latin America, and Europe. He examined the measurable value of technology capability in risk mitigation in his 2011 book *Webify*, and has served on the board of a public investment trust and on the senior executive committee of a $5B Nasdaq company.

Andrew Patterson — Chief Operating Officer

Andrew Patterson leads the delivery and optimization of ArxNimbus's cyber and AI risk-management solutions, drawing on a career that bridges public service and the private sector. In government, he served as Deputy Chief of Staff and Global Risk Advisor at the U.S. Department of Energy and as liaison to the National Security Council, shaping risk-management strategy at the highest levels of decision-making. In the private sector, he worked with PwC's Research and Insights team analyzing emerging global risks, and with leading hedge funds and commodity traders navigating complex operational and portfolio risk. Across decades of practice, he has pioneered approaches to emerging-threat analysis, cyber strategy, and enterprise risk frameworks that marry the tactical with the strategic.