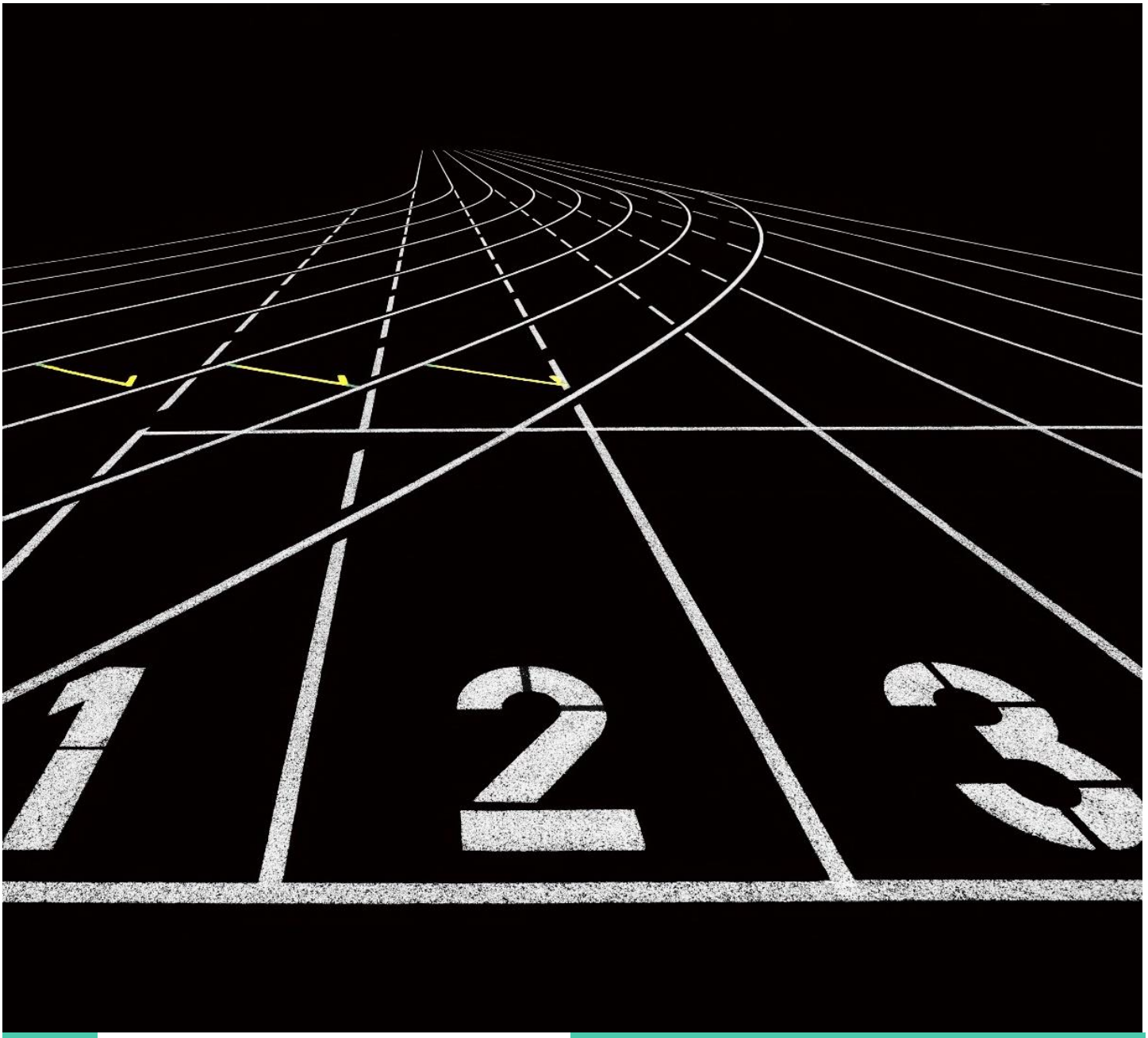
Cybersecurity Risk Management:
CONSEQUENCES OF LEGACY METHODS

ARXNIMBUS | ERDADICATE CYBER RISK info@arxnimbus.com



MANY ORGANIZATIONS ARE STILL STRUGGLING WITH OUTDATED CYBER RISK MEASURES.

Organizations that continue to rely on **legacy methods** like risk registers, pen tests, and annual risk assessments are exposing themselves to significant—and often underestimated—cyber risks. In this white paper, we explore why this happens, the often-damaging costs, and what can be done to move forward.

CONSEQUENCES OF LEGACY METHODS

Many organizations still believe that perpetuating legacy risk management methods in cybersecurity is acceptable. Companies like **Equifax**, **AT&T**, **Change Healthcare**, and **Marriott**—representing billions in losses—are stark examples. What did they have in common? A risk management "strategy" centered on three outdated measures:

- Risk Register
- Recurring Pen Tests
- Annual "Risk Assessment" by external consultants

On the surface, these measures seem reasonable, but they date back to the 1990s – *and 25 years is a very long time in technology*. Meanwhile, cybersecurity threats have evolved at an alarming pace. Even organizations that have invested heavily in advanced technologies to manage sophisticated cyber threats and vulnerabilities of today's world are still attempting to rely on outdated 1990s methods for cybersecurity risk management.

The question is: Why are organizations complacent, especially in this critical area?

The likely answer is inertia—a lack of will by decision-makers to stay current.
Often, people act when they fully understand the magnitude of a problem. So, how well do organizations grasp the risk they're facing? One way to measure this gap is by examining the risk-reducing actions companies have taken, especially after a cyber event.

A Glaring Example: Equifax

Equifax's total documented losses from its 2017 breach exceeded **$1.4 billion**. Yet, how much insurance did they have? Just **$40 million**—covering only **2.86% of the loss**. More than **97%** of the damage was uninsured and borne by the company and its shareholders.

A Healthcare Sector Struggle: Change Healthcare

In **February 2024**, Change Healthcare, a UnitedHealthcare subsidiary, suffered a **ransomware attack**. The projected losses exceeded **$4 billion**, with some estimates reaching **$6 billion**. However, the company had only **$100 million** in cyber insurance coverage—covering just **1.67%** of the loss.

Underestimated Risks: A Common Thread

Other companies show a similar pattern of under-insurance, leaving shareholders, customers, and employees to bear the brunt of the losses. This raises significant governance concerns: could management have intended to under-insure? If so, proper governance demands transparency so shareholders can weigh the implications of such exposure.

But if under-insurance isn't intentional, then it's likely due to an **underestimation**—a massive one—of the real risks faced by these organizations. Could these companies, relying on outdated legacy methods, have miscalculated their cyber risk by such catastrophic amounts?

Let's take a deeper look at these **legacy methods** to understand why they may fail in today's fast-paced cybersecurity landscape.

The Outdated Risk Register

Risk Register technology has been around since the late 1990s. **Tom Kendrick** highlighted the use of risk registers in his 2003 book on project management, where risks were identified based on expert opinions and documented

for future tracking. While risk registers may be valuable for capturing risks, they are inherently limited by the collective imagination of those involved in the process.

Imagine a NASA launch where the risks are identified by going around the room and asking launch control officers, rocket technicians, and perhaps even the astronauts themselves questions like "what do you think are our greatest risks?" The answers are then documented in a spreadsheet-like database, including everyone's expectation of loss. Should this be relied upon as the primary source of anything approaching truth about something as serious as cybersecurity risk? It's simply **not feasible** to rely solely on subjective opinions when dealing with something as critical as cybersecurity.

For instance, when a **Fortune 20 global company** with 48,000 employees listed only **64 risks** in its cybersecurity risk register, it was clear during my debriefing to the leadership that this approach did not provide a complete picture. While part of the cybersecurity practice at PwC, I personally led the implementation of risk registers on more than one occasion. Given today's cyber threat landscape, where sophisticated attacks can originate from nation-state actors or automated **AI-driven systems**, relying on a method developed in the 1990s falls far short of what's needed.

Pen Testing: A Necessary but Insufficient Measure

Penetration testing, or **pen testing**, has its roots in work done by the RAND Corporation in the 1960s and became widely used by the 1980s. While it remains a valuable technique for identifying vulnerabilities, it was designed in an era when threats were far less complex than today's landscape.

In the 2020s, pen testing has been outpaced by the rise of **machine-to-machine attacks** and **nation-state-sponsored cyber threats**. These sophisticated adversaries deploy weapons-grade technology in industrial-scale operations, far beyond what a pen tester team can replicate.

> ***Fact:*** *According to a **2023 study by Cybersecurity Ventures**, the global cost of cybercrime is projected to reach **$10.5 trillion annually by 2025**, driven in part by sophisticated automated attacks.*

Annual Risk Assessments: Too Little, Too Late

Annual risk assessments, another relic of the 1990s, are often conducted by consulting firms, many of which apply audit discipline to their assessments. While these assessments can reveal vulnerabilities, the process is inherently flawed due to its **static nature**. Cyber threats evolve at lightning speed, and an annual snapshot simply cannot keep pace with rapidly changing threat vectors.

Moreover, most risk assessments fail to quantify the **financial impact** of cyber risks. They often exclude critical areas such as **shadow IT, cloud risk, IoT**, and **third-party risks**, which leaves organizations vulnerable to massive blind spots.

> A **2024 report by Gartner** revealed that **40% of organizations** with annual risk assessments overlooked at least one critical vulnerability in their **IoT** infrastructure.

So, what we have is a picture that looks something like this:

Legacy method	Origin	Framework-adherent?	Threat classification?	Financial Rendering of Risk?
Risk Register	1990s	N	N	Partially
Penetration Testing	1960s	Potentially	N	N
Annual Risk Assessment	1990s	N	N	N

A Shift Toward Actuarial Science in Cyber Risk Management

As legacy methods falter, the **insurance industry** has adopted more rigorous actuarial methods to assess risk, moving beyond subjective judgment-based methods. These actuarial approaches quantify risks with precision, allowing for better underwriting of cyber insurance policies. Without actuarial science, insurance providers can't establish accurate premiums to cover the risk they're taking on.

Today, leading enterprises are adopting **actuarial models** to guide their cybersecurity risk management efforts. This shift allows companies to:

- Determine the appropriate level of insurance coverage
- Inform remediation strategies
- Justify cybersecurity budgets based on data, not opinion
- Optimize their risk management approach

Fact: According to a **2023 Deloitte study**, companies that adopted actuarial methods saw a **25% reduction in cyber insurance premiums** and improved their overall risk posture.

CONCLUSION:
THE FUTURE OF CYBER RISK MANAGEMENT

Organizations that continue to rely on **legacy methods** like risk registers, pen tests, and annual risk assessments are exposing themselves to significant—and often underestimated—cyber risks. The rise of **actuarial science** in cyber risk management offers a clear path forward, allowing organizations to accurately measure, mitigate, and insure against today's threats.

As cybercrime becomes more automated and sophisticated, businesses must evolve their risk management practices. The days of relying on outdated methods are over. Forward-thinking companies will embrace data-driven models to safeguard their future.

ABOUT THE AUTHOR

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.

ABOUT ARXNIMBUS

Founded in 2016, ArxNimbus set out to revolutionize cybersecurity by applying actuarial quantitative risk management to digital risk exposure for organizations of all sizes. Under sponsorship of US Strategic Command, ArxNimbus developed the patented Thrivaca™ Risk Profile—the only NIST-approved solution for generating a financial rendering of comprehensive cyber risk exposure. With Thrivaca, organizations can enhance their existing risk management strategies, recover costs, reduce unfunded liabilities, tackle tech debt, and minimize litigation risks—all while securing vital management support for cybersecurity investments.

Trusted by enterprises and cyber insurers alike, ArxNimbus delivers accurate, actionable insights, verified by researchers, actuaries, and economists. Recognized as a veteran-owned, Gartner Peer Insights Cool Company and honored by Pepperdine University as a Most Fundable Company, ArxNimbus is also celebrated as one of the top cybersecurity innovators by Momentum Partners' Cyberscape.

Don't wait until it's too late. Partner with ArxNimbus to proactively protect your organization, reduce litigation exposure, and gain the peace of mind that comes from knowing your cyber risks are fully understood and managed.

Let's take the next step toward a secure digital future—together.

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

Connect with us: