The Science of AI Risk Exposure

ArxNimbus

AI projects hold great promise for nearly every organization. Revenue expansion. Cost recovery. Major efficiency gains. Yet all these benefits hinge on the operational assurance and sustainability of our AI efforts. Are we doing what's necessary to assure the intended results? In your business it's crucial - the risk is real, and it's all around us and growing. But how much do we know? Being able to map, measure, manage and govern these increasingly-vital AI functions is critical, in order to maintain and expand these valuable gains.

"I don't think the world will put up anymore with any of us coming up with something where we haven't thought through safety, equity and trust - these are the big issues."
- Satya Nadell, Chariman, Microsoft

Arx Nimbus has a passion to deliver quantitative, insurance-grade AI risk understanding to every organization. Through the DoD-sponsored AIA© product, we bring real-world insight to the impact and dynamics driving cyber risk. Developed by practicing risk professionals, PhD actuaries and economists, AIA allows every enterprise to know where, why and how much AI risk is able to impact the organization, and to direct investment and effort to the areas of greatest improvement. There is simply too much at stake in today's AI investments to not get this right.

Based on a proprietary algorithm reflecting known probabilities, the actuary-designed ArxNimbus mathematical model profiles the effects of cybersecurity risk using your vulnerabilities, your financials, and your AI exposure. Now enterprise AI risks can be identified at their source. The degree and relative level of AI risk is quantified by AIA in financial terms - enabling transparency and oversight for each AI initiative, and the NIST-approved guideposts for risk reduction.

By conforming with NIST standards including the NIST AI-RM framework, AIA supports the detailed examination and analysis of AI risk at its source. Availability, Access, Abuse, Integrity and Model Privacy Data are quantified based on the current controls and practices in place. Multiple AI intiatives, typical of most organizations today, can be evaluated as an overall AI portfolio of projects.

Understanding AI Risk

How does management currently select the best AI assurance options and capabilities for the organization? Often, these decisions were made based on professional judgment or expert opinion. Over time, experience and litigation have caused an aversion to personal opinion as a basis for a strong cybersecurity program. Just as no modern airline would operate aircraft based on pilot judgement alone, so AI is proving too vital to leave to the risks associated with human error.

Using the detailed definitions of accepted audit standards, controls, and regulatory requirements, AIA uses the inter-relationships of the key factors of threats, risks, vulnerabilities and capabilities to properly measure the effects of each area of the cybersecurity program on risk. Using the common language of mathematics and finance, AIA makes visible the effects of the vital decisions around investment, risk tolerance, model protection, insurance, and capability that simply must be gotten right.

"Success is creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks."
- Stephen Hawking, Theoretical Physicist, Cosmologist, Author

Key Questions to Ask

- *How do I gain a real assessment of risks within my current AI initiatives?*
- *What are my top AI risks, and what is their relative financial impact?*
- *What is the value of addressing certain specific AI vulnerabilities?*
- *How can I chronicle my efforts at AI risk reduction interms that put me on my best footing for compliance, regulatory, and legal preparedness?*
- *How can I properly forecast the probabilities of certain AI scenarios?*
- *What is the value to the enterprise of AI-risk insurance?*
- *How do we gain common direction and agreement among senior management to confidently support awell-targeted AI assurance program?*

AIA focuses on whole-enterprise cybersecuritystatus and quantitatively analyzes this data against prevailing regulatory frameworks to answer these and other key questions - with results in just 48 hours.

"Without proper controls, AI systems can amplify, perpetuate, or exacerbate inequitable or undesirable outcomes for individuals and companies."
- NIST, January 2023 (https://doi.org/10.6028/NIST.AI.100-1)

About ArxNimbus

Arx Nimbus radically advances how companies understand and optimize their cybersecurity program. Our passion is to bring real, actionable knowledge of cybersecurity risk to enterprise, investors, advisors and insurers worldwide. Thrivaca was designed using fact-based, mathematically modelled analyses of the cybersecurity landscape. Arx Nimbus applies the Thrivaca platform to model and evaluate the effects of Capabilities, Threats and Vulnerabilities on Cybersecurity Risk, and is the sole provider of the NIST-based AIA risk management platform for today's AI initiatives.

Leaders seldom know how to anticipate and evaluate the impact of undefined risk. Bridging this gap, ArxNimbus uses threat analysis, automated scanning, regulatory standards, vulnerability data and probability algorithms and digital twin technology to bring insurance-grade quantitative models to properly gauge the financial impact of likely outcomes based on alternative optional strategies. Knowing the financial meaning of your options and strategies lets every organization prioritize and invest with greater confidence and precision.

Category	Control	Control Status (Scale 1-5)	Financial Exposure
Manage-1: AI risks based on assessments and other analytical output from the Map and Measure functions are prioritized, responded to, and managed	Manage 1.1: A determination is made as to whether the AI system achieves its intended purpose and stated objectives and whether its development or deployment should proceed	3.10	$ 70,000
	Manage 1.2: Treatment of documented AI risks is prioritized based on impact, likelihood, or available resources or methods.	1.80	$ 144,000
	Manage 1.3: Responses to the AI risks deemed high priority are developed, planned, and documented	2.20	$ 1,600
	Manage 1.4: Negative residual risks to both downstream acquirers of AI systems and and users are documented	3.70	$ 428,000
Manage-2: Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, and documented, and informed by input from relevant AI actors.	Manage 2.1: Resources required to manage AI risks are taken into account, along with viable non-AI alternative systems, approaches, or methods to reduce the magnitude or likelihood of potential impacts	3.00	$ 7,900
	Manage 2.2: Mechanisms are in place and applied to sustain the value of deployed AI systems	2.50	$ 81,000
	Manage 2.3: Procedures are followed to respond to and recover from a previously unknown risk when it is identified	3.60	$ 12,413

Who cares about AI Risks?

Regulators Care
- Compliance
- Disclosure
- Ever-expanding requirements

Shareholders Care
- Enterprise value
- Litigation exposure

Management Care
- Risk Management
- Exposure of brand
- Shareholder equity at risk
- Costs of non-compliance
- Costs of breach

Customers Care
- Perceptions of safety and security of customer data
- B2B third-party risk

www.arxnimbus.com info@arxnimbus.com 888-422-6584