A New Approach to Thirdparty Threat Exposure Management™

The RiskOpsAI™ Thirdparty Threat Exposure Management™ (TTEM™) offers an AI driven continuous and predictive approach to third party threat-risk exposure management, supporting effective risk decision-making and driving business success.

- Organizations carry significant threat-risk exposure in today's rapidly changing operational and technology landscape, where predicting and minimizing the impact of multiple thirdparty threat-risks (including cyber, data privacy, compliance and ENISA's NIS2) can be challenging.
- The current tactical approach to third party threat-risk exposure management (reactive, siloed, periodic and piecemeal) fails to connect the impact of risk to an organization's business goals and objectives.
- Aggregating thirdparty threat-risk exposure data from multiple vendors and suppliers to create a High Fidelity Single Source of Truth™ is a threat-risk exposure management imperative when seeking to eliminate blind spots and reduce exposure.

Multi-Dimensional Thirdparty Threat Exposure Management™

Unique RiskOpsAI™ Native "inside out" modeling delivers continuous threat-risk assessments, risk quantification and risk prioritization (including scenario planning) across multiple thirdparty risks, including cyber, data privacy, compliance and NIS2. The platform provides detailed drill down analytics (by risk) for each Thirdparty Supplier, including risk exposure, as follows:

- Cyber: e.g., Trophy penetration, ransomware, identity access risks.
- TPRM: e.g., Physical / Geopolitical / Financial, Geo-logistic / supply risks.
- Services: Insider breach, privacy disclosure, security, and technology debt risks.

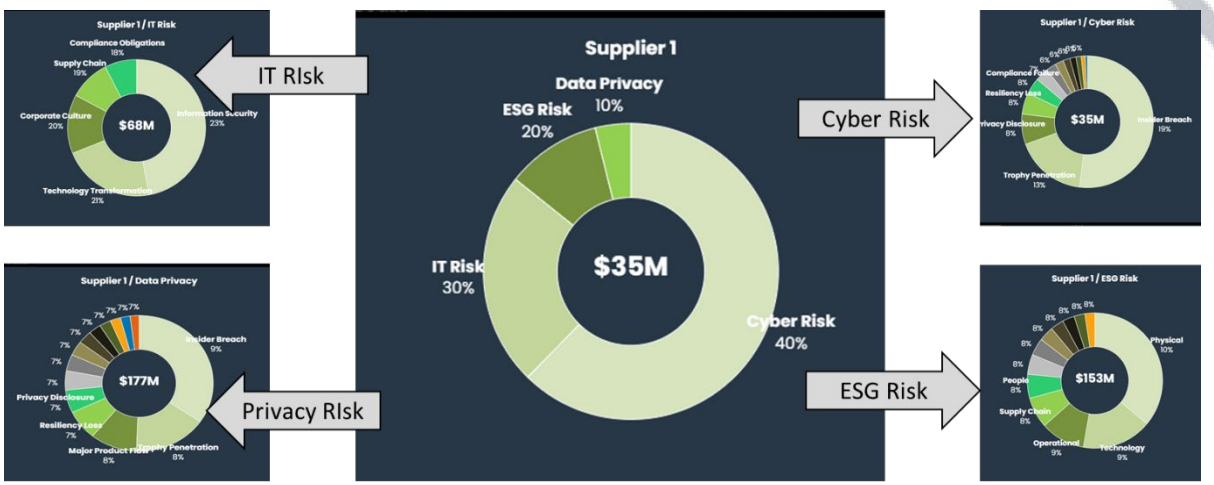

Figure 1

A Comprehensive View of Thirdparty Threat Exposure

The RiskOpsAI™ solution provides an organization-wide view of thirdparty threat-risk exposure by multiple risk criteria. Rank Stacking of third-parties by threat-risk type, risk exposure, location and risk remediation cost supports intuitive risk mitigation decision-making and Threat-Risk Exposure Tiers.

Figure 03

Each third-party threat-risk criterion can be further drilled down to understand key risk factors negatively impacting the organization.

The AI/ML powered multi-dimensional thirdparty threat-risk exposure architecture can draw from a common inventory of controls across cyber, data privacy, compliance and TPRM risk frameworks. Our Risk Common Control Model™ can be generated to support the unique third-party threat-risk exposure characteristics of any organization.

AI Native Thirdparty Threat-Risk Exposure Analytics

The RiskOpsAI™ driven TTEM™ platform generates dashboards that are highly configurable for multiple personas and use cases. Furthermore, each dashboard is highly customizable and can be used for multiple purposes and roles to generate a wide range of thirdparty analytics.

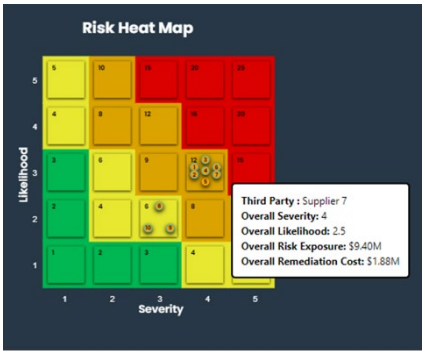

Figure 02

The risk heat map, for example, shows Likelihood and Severity by risk exposure. Each third party's overall threat-risk exposure can be mapped to contributing risk factors, including cyber, data privacy, compliance, and DORA. Meaningful dashboard insights minimize negative events, gain support for resources and support business goals.

About OptimEyes AI® d.b.a. RiskOpsAI™ (Risk Operations Using AI™)

San Diego-based OptimEyes AI® doing business as RiskOpsAI™ known as the Integrated Risk Modeling & Decisioning® Company, is a pioneer of AI Native, IRMR methodologies. Built by cyber, risk, and compliance veterans, our software-as-a-service (SaaS) platform helps Fortune 2000 organizations discover, measure, prioritize, predict, and optimize cybersecurity, data privacy, and enterprise risks. For more information, contact us at info@optimeyes.ai, and visit https://optimeyes.ai, and follow us on:

**** For a No Obligation Risk Assessment evaluation, please contact: sales@optimeyes.ai***