Holistic, Repeatable Risk Quantification and Loss Estimation

There’s always a new frontier that organizations need to be prepared to deal with. The latest is the emergence of the cyber domain, which means businesses are working to proactively identify, quantify and manage cyber risks.

However, the constantly evolving risk landscape, coupled with the limitations of qualitative assessments, results in few organizations having a comprehensive understanding of their cyber risk exposure.

Risk quantification can help you effectively focus your cyber risk management efforts. Optiv’s tailored approach leverages a cyber risk quantification framework based on the industry standard Factor Analysis Information of Risk (FAIR) model, providing a business-centric, repeatable method that evaluates cyber risk factors and loss estimates in financial terms for cyber risk scenarios applicable to the business.

Optiv Solutions

Optiv’s differentiated approach to cyber risk quantification enables organizations to choose the engagement path most closely aligned with their stated business, technology and risk management objectives. Our experience, framework and accelerators (industry baselines, threat vulnerability mapping and capability control mapping) can add value to your existing risk management paradigms and help you build an in-house risk quantification capability.

We combine a comprehensive understanding of cyber risk and leading practices with your business objectives, resulting in the delivery of personalized solutions that help quantify risks in monetary terms and empower leadership’s investment decisions.

Cyber Risk Quantification Methodology

**PHASE 1: BUSINESS PROFILING**
- Understand business objectives, priorities and crown jewels through stakeholder interview and roadmap review.
- Review the coverage of existing risk register and document vulnerabilities impacting the identified priorities integrating cyber risk with business risk.

**Results:** Business objective and crown jewel identification, updated risk register.

**PHASE 2: RISK SCENARIO SCOPING**
- Finalize risk scenarios applicable to business based on risk register and threat landscape.
- Determine magnitude of impact to the business from risk scenarios through stakeholder workshops.

**Results:** Tailored risk scenarios, risk impact assessment.

**PHASE 3: INDUSTRY BASELINING**
- Tier the target organization as per the applicable industry sector and revenue band.
- Collate emergent industry trends to identify and apply threat likelihood and financial impact of risks based on industry and cohort information.

**Results:** Likelihood of risks, understanding of financial impact.

**PHASE 4: QUANTIFICATION DASHBOARDING**
- Determine probabilities of occurrence and range of potential losses for the identified risks.
- Develop risk quantification dashboards and organization level risk report.
- Leverage findings to prioritize investments, identify mitigation plans to bring down risk and loss estimates.

**Results:** Financial quantification dashboards, investment priority and mitigation plans.
Our novel cyber risk quantification framework enables a collaborative understanding of cyber risk in alignment with your business objectives and goals.

**Case Study**

**Fortune 100 Technology Manufacturer**

**DESIRED OUTCOMES**
A large technology company wanted to develop their risk quantification program and align risk reduction efforts based on their return on investment.

**SCOPE**
The client’s complex environment consisted of multiple business units and wanted to better understand and enumerate their risk exposure across the various business units and security offices.

**SOLUTION**
Optiv used its industry-leading cyber risk quantification framework to provide the client with a repeatable method to evaluate, quantify and describe risks in understandable financial terms. We leveraged specific loss scenarios applicable to the organization to analyze and report on potential loss estimates that could impact the company based on their current security capabilities.

**CLIENT BENEFITS**
Our tailored approach allowed the client to combine qualitative and quantitative inputs to allow for the expression of cyber risks in financial terms. Optiv created an organization-level risk report describing the portfolio of identified risks in monetary terms and leveraged those findings to prioritize investments, streamline plans and improve overall risk-readiness.

---

**The Optiv Advantage**

- **10+ Years** - Average team member’s industry experience
- **Public and private industry expertise** – federal, state and local government, finance, technology, manufacturing, retail, critical infrastructure, travel and leisure, healthcare, insurers, communications, media, transportation and more
- Our team has had speaking roles on cybersecurity best practices and due diligence at numerous industry conferences, including:
  - The Cloud Security Alliance
  - The RSA Security Conference
  - Speaker tracks at OptivCon, Optiv’s own security conference
- Support for numerous blogs, articles and white papers

---

**Secure greatness™**

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.