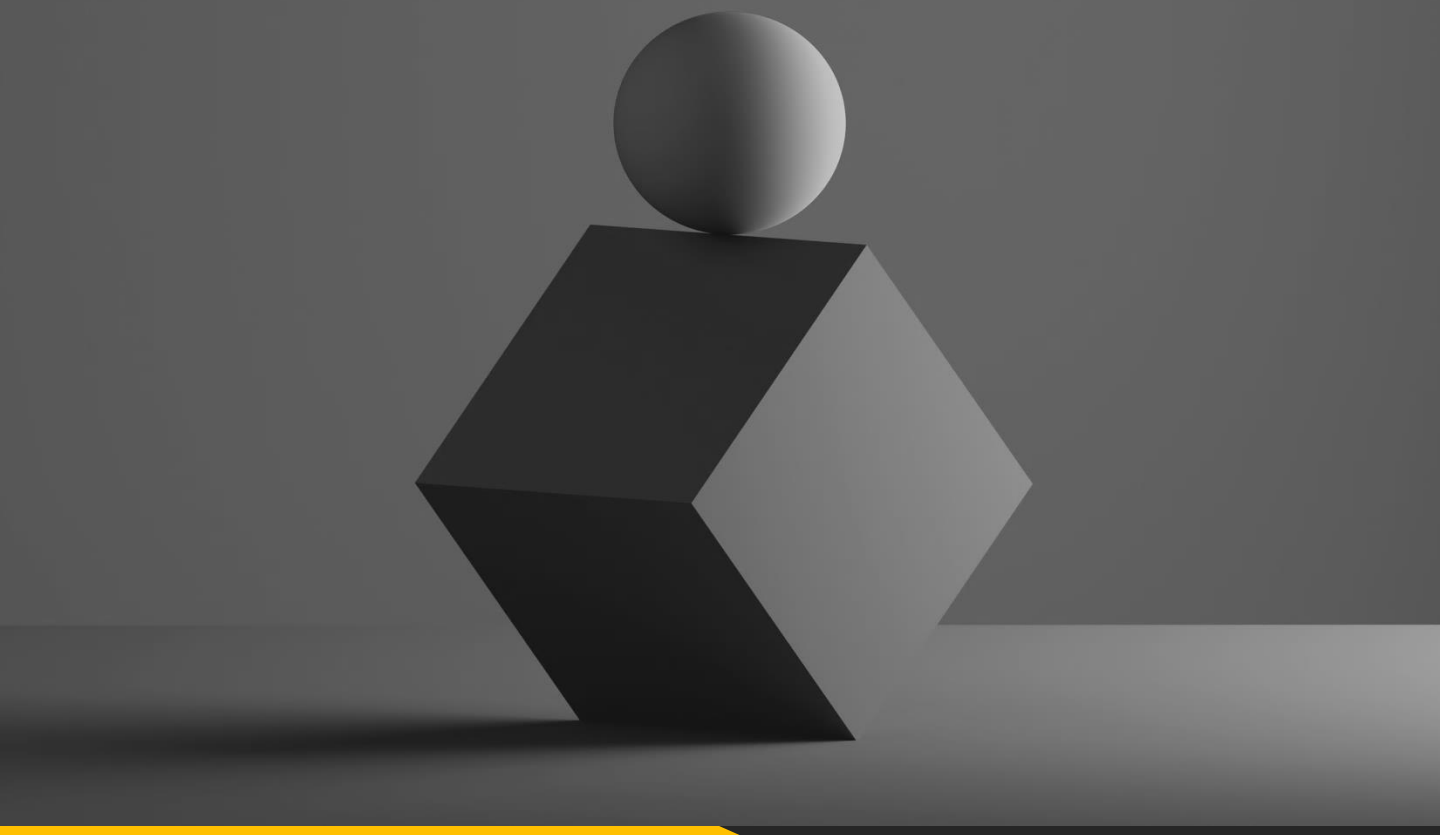
Proton Technosoft
Securing your digital footprints !!

CYBER RISK QUANTIFICATION

POINT OF VIEW



www.protonts.in

In the increasingly interlinked digital world of today, cyber threats are no longer the topic of speculation—but facts of life—real, driven, and potentially destructive ones.

With data breaches and ransomware infections, the effects of cyber incidents can be measured not only in technical disruption but also in reputational damage, legal risk, and financial loss. Navigating this high-risk environment entails transitioning from reactive risk management to quantitative risk analysis—the mainstay of the new-age cybersecurity agenda.

Cybersecurity risk quantification process assigns measurable values to probable threats to answer two main questions:

1. What is the likelihood of the threat happening?
2. How would it be impacted if it does?

This process moves businesses from educated, qualitative guesses (e.g., “high”, “medium”, “low”) towards data-enabled models amenable to better decision-making.

Risk Quantification Benefits !!

Risk Prioritization

Quantification lets you remediate based on risk impact—instead of severity scores. You don't necessarily want to remediate the 9.8 CVSS first if the asset is locked down.

ROI Realization

By expressing threats in financial language, CISOs can present the board or CFO with a strong business argument.

These quantified Risk profiles allows organizations to determine right amount of cyber insurance coverage and thereby rationalizing the premiums fuelled by data.

Business Recovery

With Quantification of Risk, SLA's can be assigned to security incidents and prioritized actions can be taken to recover the business based on its impact, leading to pragmatic and proven business continuity plans.

Further, measurable risks can be expressed in business-friendly language, bridging the divide between CISOs and the leadership team.

Benchmarking

It enables risk trends to be tracked over time, by looking at likelihood and quantified impact trending month on month, or year on year.

This trend analysis provide a vital insight into the control strength improvement over time and aids in continuous maturity improvement.

Common Risk Quantification Approaches

F.A.I.R

Uses a structured taxonomy to quantify cyber risk in monetary terms

- Breaks down risk into Loss Event Frequency (LEF) and Loss Magnitude (LM).
- Quantitative and scenario-based
- Widely adopted in Fortune 500 companies
- Supports decision-making and ROI evaluation

CVSS + Asset Valuation

Combines Common Vulnerability Scoring System (CVSS) scores with asset criticality and business value.

- Produces semi-quantitative risk ratings.
- Simpler to implement
- Common approach in vulnerability management and security operations
- Lacks probabilistic measure
- Not a true financial quantification

Monte Carlo Simulations

Uses probability distributions and runs thousands of simulations to estimate potential loss.

- Outputs a range of possible losses with associated probabilities.
- Often used with frameworks like FAIR.

Challenges in Quantification of Risk

Requires accurate data

Needs cross-functional input

Perceived as time-consuming or complex

Need cultural alignment

Conclusion

Risk quantification is no longer simply a technical exercise—a business imperative. In times when cyber incidents can halt operations, corrupt trust, and gain the attention of the regulatory community, enterprises must adopt a formal and quantitative approach of knowing, prioritizing, and managing cybersecurity risk.

By infusing risk quantification into governance and security procedures, organizations can shift from reactive defence to proactive resilience—so that cybersecurity is no longer simply a cost center, but also an enabling strategic one.