## Documents

Ghosh, K.

**Identification and Quantification of Cybersecurity Risk by Likelihood-Severity, Incident-Response and Organizational Asset Valuation Framework**
(2020) *SSRN*, .

**DOI:** 10.2139/ssrn.3630075

Vinod Gupta School of Management, Indian Institute of Technology Kharagpur

**Abstract**
With the business disruptive translation of IT systems and networks, Cyber (Cybersecurity)-Risk has increased manifold over the past decade. The Zero-day attacks are now common phenomena. Tightening of security controls are not strictly sufficient to contain cyber security risks and to combat cyber warfare. Establishing threat intelligence platform and cyber-risk analysis, prevention and mitigation within an organization is now becoming indispensable for organizations to perform. This paper identifies the requirement of quantification of cyber security risks and further delves into cyber risk quantification methods by proposing qualitative and quantitative approaches for quantifying, equating and calculating cyber-risk. The paper further proposes three frameworks i.e., Likelihood-Severity, Incident-Response and Organizational Asset Valuation Framework to identify and quantify cyber-risk and risks associated with information infrastructure. It is held that Identification, Earmarking and Valuation of business critical assets, systems and information strive towards risk reduction, mitigation and operational excellence. 

**Author Keywords**
Cyber-risk; Cyber-risk analysis; Incident-Response; Likelihood-Severity; Organizational Asset Valuation Framework; Risk quantification; Zero-day attack

**Correspondence Address**
Ghosh K.; Vinod Gupta School of Management, email: kaushikghosh@iitkgp.ac.in

**Publisher:** SSRN

**ISSN:** 15565068
**Language of Original Document:** English
2-s2.0-85110544331
**Document Type:** Preprint
**Publication Stage:** Final
**Source:** Scopus