Cyber Risk Management - Research Proposal

Rishit Saiya (CSCI 530)

The threat of information security incidents is climbing. Risk management authorities must consider their mitigation strategy in relation to the state-of-the-art threat landscape, existing security frameworks and global regulations to strategically manage these risks.

With the rapid increasing threats of information security, I intend to cover the prevalence, complexity and severity of high-risk attacks. According to latest reports, headlines have demonstrated a very high varied spectrum of attack methods. as well as the accompanying reputational damage.

Today’s growing network of connectivity only increases information risk, leaving organizations exposed and unprepared. This culminates to a massive Reputational, Technological damage and leading debt. This culminates the conglomerates to go through an ever-lasting impact of breach, legal liabilities, audit, probation, financial fines and deficit.

Due to above factors, few organizations have now started to take step towards handling information security incidents. As the second line of defense against information risk, ERM (Enterprise Resource Planning) is responsible for overseeing and mitigating risk. Risk management authorities are now assessing the threat landscape. Based on risk factors, risk authorities submit their assessment to higher management. This helps the critical decision takers to allot their financial and infrastructural resources to security flaws based on their risks whilst considering which information security framework fits best into their organization’s operations and strategy. Recent government regulations and compliance has become stringent which essentially asks the organizations to release breach disclosures on public records.

I intend to survey through the following research articles, public documents and government compliances.

References:

1. Risk Management: Coordinating Corporate Investment and Financing Policies [[Link](https://onlinelibrary.wiley.com/doi/full/10.1111/j.1540-6261.1993.tb05123.x)]
2. Reducing Informational Disadvantages to Improve Cyber Risk Management [[Link](https://link.springer.com/article/10.1057/s41288-018-0078-3)]
3. A Framework for Using Insurance for Cyber-Risk Management [[Link](https://dl.acm.org/doi/abs/10.1145/636772.636774)]
4. Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies [[Link](https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12844)]
5. Protecting Controlled Unclassified Information in Non-federal Systems and Organizations [[Link](https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final)]
6. NIST Risk Management Framework [[Link](https://csrc.nist.gov/projects/risk-management/about-rmf)]