

Case ID:M23-249P^

Published: 3/18/2024

Inventors

Stefano Chiaradonna

Petar Jevtic

Nicolas Lanchier

Sasa Pesic

Contact

Physical Sciences Team

Cyber Risk Loss Distribution Model of Client-Server Networks

Cyber risk has emerged as a significant threat to businesses that have increasingly relied on new and existing information technologies. Across various businesses in different industries and sectors, a distinct pattern of IT network architectures, such as the client-server network architecture, may expose those businesses, which share it, to similar cyber risks. Recent cyberattacks have exhibited the capability to disrupt business operations and cause permanent data loss resulting in significant financial losses to a business. To mitigate such losses, risk managers and decision-makers continuously make decisions that stem from questions on how best to protect their business's IT network.

Risk management and decision-makers increasingly face decisions that stem from the following questions: How does the cybersecurity protection of my business's information technology systems impact my losses? And, what price-effective investment strategies in cybersecurity protection help reduce my potential liabilities? To have clear cyber risk assessments and make informed decisions on investments in cybersecurity protection on a fixed budget, risk managers need frameworks that account for their IT networks and unique cybersecurity environments. Thus, there is a need for a model for aggregate loss distribution for cyber risk (i.e., quantifying cyber risk).

Researchers at Arizona State University have developed a contagion model to characterize the microscopic properties (mean and variance) of previously unknown or not fully known empirical distribution of losses resulting from a cyber-attack on a client-server network. The model computes the exact mean and variance of the cyber risk loss distributions depending on key parameters such as probabilities of attack types, the topology of the network of clients, and contagion strength. This model can also provide insights into better strategies for cybersecurity protection on a client-server network. For example, risk managers can use this model to have clear risk assessments and make informed decisions on investments in cybersecurity protection on a fixed budget.

Related publication: [Framework for Cyber Risk Loss Distribution of Client-Server Networks: A Bond Percolation Model and Industry Specific Case Studies](#)

Potential Applications:

- Client-server network users
- Risk management professionals
- Cyber security insurers

Benefits and Advantages:

- Unique, novel model of an aggregate loss distribution for cyber risk

- Insights into better investment strategies for cybersecurity protection
- Model has been applied to four case studies: implantable medical devices, smart buildings, ride-sharing service, and vehicle-to-vehicle cooperation in traffic management