Skysong Innovations
Advancing the Arizona State University Knowledge Enterprise

1475 N. Scottsdale Road, Suite 200
Scottsdale, AZ 85287-3538
Phone: 480 884 1996 Fax: 480 884 1984

Case ID:M22-229P^
Published: 4/5/2024

Inventors

Stefano Chiaradonna
Petar Jevtic
Nicolas Lanchier

Contact

Physical Sciences Team

Cyber Risk Loss Distribution of Hospital Infrastructure

Networks like those of healthcare infrastructure have been a primary target of cyberattacks for over a decade. From just a single cyberattack, a healthcare facility would expect to see millions of dollars in losses from legal fines, business interruption, and malpractice lawsuits. As more medical devices become interconnected, more cyber vulnerabilities emerge resulting in more potential exploitations that may disrupt patient care and result in catastrophic financial losses. In particular, for eleven consecutive years, the healthcare industry incurred the highest average data breach cost, where data breaches are defined as confirmed security events that compromised the integrity, confidentiality, or availability of data by an unauthorized party.

Data breaches are only one consequence of a cyberattack. A cyberattack, especially ransomware which is designed to disable devices until a ransom is paid, is rampant in targeting hospitals. Ransomware attacks cripple vital systems and prevent hospitals from accessing important patient data that can impede or halt operations from hours to months. This epidemic of cyberattacks and the resulting consequences within the healthcare industry have shown no signs of slowing down or decreasing in severity. These attacks disrupt hospital operation and patient care even after the contagion is contained. There is a need for a cyber security risk assessment model that quantifies loss from a cyberattack in a hospital setting.

Researchers at Arizona State University have developed a loss model for a mixed random network (e.g., a prototypical hospital) with a contagion spreading throughout the internal network. The results of this model provide analytical results and their numerical implications related to the mean and variance of the aggregate loss distribution. This model paves the way for insurers to price cyber risks on mixed random networks (e.g., hospital infrastructure). The model is effective with various sizes of hospital networks and allows for diverse cybersecurity measures.

Related publication: Framework for cyber risk loss distribution of hospital infrastructure: Bond percolation on mixed random graphs approach

Potential Applications:

- Insurers (e.g., for cyber insurance policies, for pricing cyber risk, etc.)
- Healthcare administrators
- Cyber professionals (e.g., for risk assessments)

Benefits and Advantages:

- Assess expected financial losses due to a cyberattack on a micro level of an organization’s network

- Considers bidirectional connections in a hospital's network (i.e., the spread of malware within a hospital due to the variability of interconnected devices)
- Provides a tool to model a cyberattack on a hospital's internal network and to yield the associated loss distribution for insurers, hospital administrators, and cybersecurity professionals