

**M E M O R A N D U M**

DATE: 08/12/2024

TO: Faculty and Students

FROM: Professor(s) Petar Jevtic and Nicolas Lanchier  
Chair/Co-Chairs of Stefano Chiaradonna  
Defense for the PhD in Applied Mathematics  
Committee Members Dragan Boscovic  
Sean Warnick  
Tiffany Bao

**DEFENSE ANNOUNCEMENT**

Candidate: Stefano Chiaradonna

Defense Date: Monday, September 9, 2024

Defense Time: 12:30 PM

Virtual Meeting Link: <https://asu.zoom.us/j/8115898432?omn=87982818032> or WXL Rm.113

Title: Essays on Probabilistic Modeling of Cyber Risk

Please share this information with colleagues and other students, especially those studying in similar fields. Faculty and students are encouraged to attend. The defending candidate will give a 40-minute talk, after which the committee members will ask questions. There may be time for questions from those in attendance. However, guests are primarily invited to attend as observers and will be excused when the committee begins its deliberations or if the committee wishes to question the candidate privately.

**ABSTRACT**  
**-See next page-**

## ABSTRACT

Cyber risk has emerged as a significant challenge to businesses and critical infrastructures, such as hospitals, that have increasingly relied on new and existing information technologies (IT). For purposes of pricing this emerging risk and as an aid for improved cybersecurity network hardening, three essays propose probabilistic network modeling frameworks to obtain the exact mean and variance of loss distribution characterization for various informed network configurations.

The first essay is a published paper modeling the cyber risk of a single small-and-medium-sized enterprise (SME) as a random tree with network segmentation. Lacking the resources and mature cybersecurity programs of larger organizations, SMEs struggle to protect against sophisticated cyberattacks and often purchase cyber insurance to mitigate financial losses. In this context, this essay characterizes the loss distribution for pricing purposes.

The second essay is a published paper that proposes a structural model of an aggregate loss distribution for a prototypical hospital network. Modeled as a mixed random graph, the hospital network consists of various patient monitoring devices and medical imaging equipment as random nodes to account for the variable occupancy of patient rooms and availability of imaging equipment that are connected by bidirectional edges to fixed hospital and radiological information systems. The framework accounts for the documented cyber vulnerabilities of a hospital's trusted internal network of its major medical assets. This essay develops a probabilistic graph-theoretical framework, employing a percolation model and combinatorial techniques, to compute the mean and variance of the loss distribution for a mixed random network that can be useful for healthcare administrators and cybersecurity professionals to improve cybersecurity management strategies.

The third essay proposes a probabilistic structural framework for financial loss assessments on the class of client-server network architectures with  $K$  different client types. Across various businesses in different industries and sectors, a distinct pattern of IT network architectures, such as the client-server network architecture, may, in principle, expose those businesses, which share it, to similar cyber risks. This essay investigates four applications of the client-server network architecture: implantable medical devices in healthcare, smart buildings, ride-sharing services like Uber and Lyft, and vehicle-to-vehicle cooperation in traffic management.