YUYING LI, Western University

Modelling and pricing cyber security risk

The cyber risk insurance market is rapidly developing with more products being developed that cover the potential losses attributed to cyber attacks. This requires the insurance business to have a modelling and pricing framework necessary to obtain a fair price that will enable policy issuers to fulfill their future obligations. We present a valuation framework that integrates cyber risk modelling and calibration. A regime-switching Markov model is put forward to capture the occurrences of cyber attacks. The transition probabilities of the Markov chain are governed by another hidden Markov chain representing the various states of the cybersecurity environment. Based on the stages of the cyber attack, a cyber kill chain is built. The states are firewall working, firewall fail, and antiphising fail. A cyber attack happens when there is a transition from either of the first two states to the third state. With the aid of change of reference probability measures and the EM algorithm, dynamic estimates of the model parameters are obtained. Our main point of interest is the random loss from cyber attack, which is modelled by a doubly-truncated Pareto distribution. The Vasiček model is utilized to describe the interest rate process for the discounting of losses. The premium for a cyber security insurance contract is calculated via a simulated data set based on two pricing principles. Our methodology featuring dynamic parameter estimation and flexible adjustments in modelling various risk factors widens the available tools for valuation and risk management beneficial to insurance companies and regulators.