Cyber and liquidity: modeling a complex risk

Milliman

Cyber is a new trigger for liquidity risk, CFPs and RRPs

Cyber is not a standard trigger or scenario for liquidity risk. FRBNY Staff Report № 909 identifies the linkage between cyber and liquidity: if a bank is locked out of critical payment infrastructure, it could cause impairment and even cascade into a systemic event. A cyberattack causing liquidity impairment highlights two forms of interconnectedness: technology and interbank funding. Recovery from such an attack will require coordination between InfoSec, Treasury and Risk.

Traditional models require historical data for calibration and implicitly assume that past events are indicative of future attacks. Cyber is a high velocity, evolving threat driven not only by technology, but more importantly by people or adversaries. Therefore, modeling cyber risk must do more than analyze historic events, but rather must model plausible cyberattacks that have not occurred yet, and understand the 2nd and 3rd order impacts so that decision makers can implement effective strategies.

Complex Risk Analysis "CRisALIS"

CRisALIS provides a holistic forward-looking approach to modelling how complex risks may materialize. CRisALIS is based on complexity theory and incorporates data driven analysis, expert-derived causal modelling and artificial intelligence. It learns and evolves as your understanding of the threat evolves. It:

1. Leverages qualitative and quantitative data to enhance credibility of the model and adapts to new information as it becomes available
2. Expresses the outcome in terms of its underlying drivers
3. Considers potential common drivers of the various threat vectors directly rather than requiring correlation assumptions
4. Provides real insights into how outcomes occur enabling meaningful scenario analysis
5. Incorporates Milliman's tried and tested intellectual property and proprietary methodology
6. Explains the loss distribution tail and its components

Benefits

- Analyze cyber vulnerabilities which may lead to liquidity impairment while challenging CFP assumptions
- Identify the drivers of specific outcomes, which creates the ability to optimize a mitigation strategy
- Explain non-linear relationship between risk events, including causes, triggers and potential tipping points
- Provide executive information which allows for enhancing the CFP and RRP for cyber-liquidity scenarios
- Elucidate the root causes and drivers of how failed or successful InfoSec responses are linked to managing liquidity under duress while understanding 2nd and 3rd order effects, e.g., regulatory actions, market response, losses, etc.

Key Features

1. Threat vectors which can incorporate numerous scenarios
2. Learns and adapts as the threat evolves
3. "What if" and reverse stress investigations
4. Highlights uncertainties such as strategic liquidity hoarding
5. Easy for non-modelers to engage and use