# Quantifying cyber risk: preparing for the future

Milliman

## Cyber is an adversarial risk – someone is trying to outthink you

Cyber is a high velocity, evolving threat driven not only by technology, but more importantly by people or adversaries. Traditional models require historical data for calibration and implicitly assume that past events are indicative of future attacks. 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.

Unlike standard tools, CRisALIS is a causal model that quantifies and aggregates cyber risk. CRisALIS reports are designed to facilitate executive decision making by the board and senior management while providing the cornerstone for cyber and risk professionals to create and manage mitigation programs and investments.

## Complex Risk Analysis "CRisALIS"

CRisALIS provides a bespoke holistic forward-looking approach to modelling how cyber risks may materialize as well as how to aggregate silent cyber. 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 cyber risk tail and its components

## Benefits

- Analyze either your enterprise risk or aggregation of risk across a portfolio
- 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 establishing and monitoring of the cyber risk tolerance and other key metrics in real time
- Elucidate the root causes and cumulative impact of cyber risks enabling better decision making (e.g., 2nd and 3rd order effects impacting vendor risk, control decisions, insider threats, 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. Aggregates or decomposes cyber risk by threat vectors and triggers
5. Easy for non- modelers to engage and use