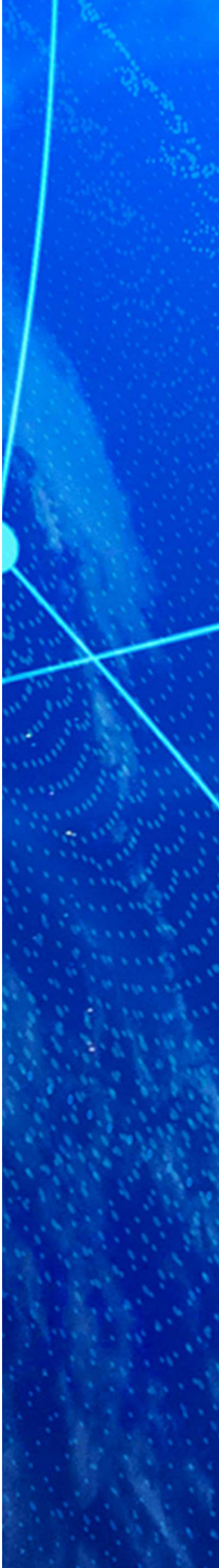
KOVRR

Cyber Decisions. Financially Quantified.

www.kovrr.com

Developing Industry Loss Curves for Cyber Insurance Using the Crimzon™ Framework

FEBRUARY 2022



The cyber insurance industry continues to grow, but it's arguably held back in terms of scale and efficiency by a lack of cyber risk quantification, aggregation and accumulation management capabilities. It can be challenging to quantify cyber for a single risk and across portfolios, which leaves insurance carriers and reinsurers struggling to secure capital to support underwriting and at risk of experiencing unexpected catastrophic and large loss events.

Cyber risk requires large amounts of data in order to fully capture the risk of significant accumulations of claims, for example: data covering the diverse array of cyber hazards, and an ever evolving view of vulnerabilities, exploits and threats. The challenge of interpreting this data into metrics which signal the level of risk is creating a barrier for insurers to secure capital and transfer risk efficiently between entities.

This issue has been tackled in the past for other classes of business by using industry loss curves, which can be used as a reference or benchmark when discussing or communicating risk. These are typically **'exceedance probability'** curves which predict the probability of an insured loss exceeding a range of thresholds.

Kovrr has developed a framework for converting the complex cyber risk and hazard landscape into a clear structure on which these curves can be built.

Kovrr's Crimzon framework[1] provides a structure on which to make sense of the millions of data points from past events, bottom-up hazard information on technologies and third-party service providers used by companies, and allows the insurance industry to get an accurate handle on potential risk and expected losses arising from catastrophic cyber events. Even players further removed in the risk transfer chain, like insurance-linked securities (ILS) funds, can use this framework to efficiently evaluate loss risk with confidence.

Crimzon™ Framework for Industry Loss Curves

Crimzon provides a structured way to map cyber risk based on **location**, **company size**, and **industry**. Companies that share these characteristics have been found through our research to have a similar profile of cyber hazards by relying on similar technologies and third-party service providers. For example:

Two large finance companies in the U.S. are more likely to share similar software, products and third party service providers. The profile of cyber hazard for these entities will differ greatly to the profile of a small scale manufacturer in Germany.

This framework allows for the risk of future cyber events to be captured in a manageable way, which is clear to understand and present, but also presents a strong risk-based approach:

- **Cyber Hazards:** By isolating groups of insured entities which will present a similar cyber hazard, we can get a clear handle on industry-wide risk and make the issue less about the individual hazards, but about clusters of common risk and security practices.
- **Major Events:** Systemic cyber events (catastrophic events) and recent supply chain related events cluster around a limited amount of Crimzon, either by targeting common vulnerabilities shared within the cohorts, or being transmitted across common chains of communication lines or dependencies.This knowledge allows us to both describe the footprint of a systemic cyber event in terms of Crimzon and model the virality/transmission between cohorts.

- **Loss Expectation:** A view of future claims can be developed by understanding the behavior and experience from past events within a Crimzon. It is reasonable to expect that risks within a Crimzon will experience similar costs and challenges responding to cyber events, so overlaying past claim frequency and severity can help develop a robust view.
- **Correlation:** Crimzon also correlates well with insurance segmentations. By understanding the common hazards within a cohort, and those shared with others, a view of correlation can be developed relatively simply. The expected loss probability can then be calculated using a manageable number of Crimzon.

Kovrr has developed this view by continually collecting data on a large number of companies within Crimzon. The data is a combination of hazards, vulnerabilities, exploits, and ground-up data on event costs, sourced from third party data and intelligence, and Kovrr's own 'Sonar 360' engine.

Using the Crimzon approach a robust structure for developing an industry curve can be presented.

Building Industry Loss Curves Using the Crimzon™ Framework

The framework above can be used as a simple framework to turn available loss and exposure data into a reliable set of loss curves, either as an exposure management tool, or for developing industry loss curves.

At Kovrr, we go a step further and use this structure together with our analysis of millions of businesses worldwide (from our 'industry exposure database') in our systemic cyber model. This generates a set of likely cyber events which will impact businesses within each Crimzon. The output is an exceedance probability (EP) curve, and a detailed year-event-loss-table (YELT), which details the cost of each event.

Systemic events are modeled by developing the footprint of an event across Crimzon, and then aggregating the losses across the zones to create a view of potential industry losses, and corresponding loss curves.

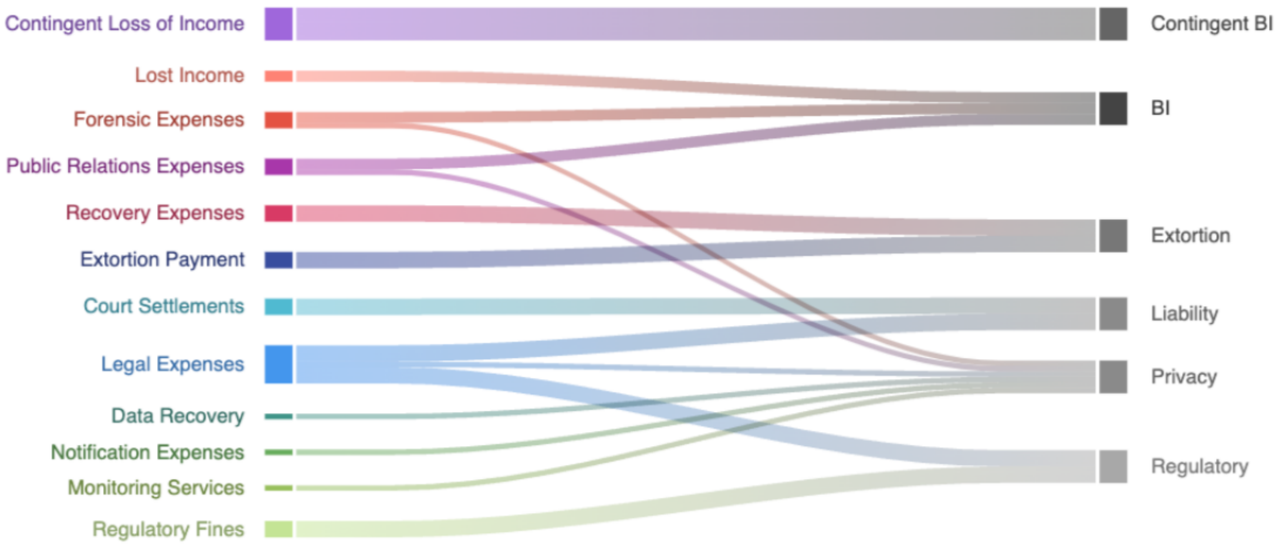
The Kovrr model captures risk on a ground-up basis, which allows us to then test the impact of changes to insurance penetration, and expectations in terms of deductible and limit profiles.

Portfolio-specific loss curves

The same approach can be taken within an insurer, and applied on a portfolio basis. This will capture specific insurance terms by policy including occurrence/aggregate limits and sublimits, coinsurance, and reinsurance terms. When capturing insurance across different regions it is important to be able to capture and map the costs incurred by the business to the correct level of insurance. A particular example would be in countries where paying ransoms is illegal and will not be covered, but in another region it is allowed.

Using the Crimzon framework, we have created a system where costs can be clearly identified and mapped to appropriate insurance coverages.

For example, we may map the costs into the following buckets, and apply sub-limits based on the coverages in each region:



Putting this data into the model then allows for more precise calculations of the risk an insurer faces within their specific portfolio, all captured in the loss curves.

Moving Forward With the Crimzon™ Framework

The Crimzon framework presents a way to build cyber catastrophe industry loss curves in a clear, efficient way. Knowing the probability of events within certain Crimzon, derived from Kovrr's extensive data collection and analysis, can then be leveraged to create industry loss curves across a portfolio or an entire industry.

Overall, industry loss curves will enable insurance companies to measure their performance and reinsurers to quantify their risk exposure very quickly while still having a meaningful degree of precision. This aggregate catastrophe cyber model does not have to be the only method for calculating risk, but it can be another powerful tool available to the insurance industry to enable efficient cyber risk transfer.

> **See how easy it can be to calculate potential cyber losses using the Crimzon framework. Get in touch with Kovrr's cyber modeling experts today.**
>
> **Kovrr financially quantifies cyber risk on demand. Our technology enables decision makers to seamlessly drive actionable cyber risk management decisions.**
>
> **Kovrr is led by an international team of (re)insurance professionals, cyber intelligence experts, catastrophe modelers, and experienced software developers.**

The Author

Peter Dyson

Insurance Modeling Specialist

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.
To learn more please contact the Kovrr team: contact@kovrr.com