KOVRR
Cyber Risk Modeling

www.kovrr.com

Importance of Insurance-Validated Risk Models to Quantify Cyber Risk

OCTOBER 2021

By its nature, cyber risk is dynamic. New events happen and evolve all the time, making it difficult for enterprises to financially quantify cyber attacks. Around two years ago, for example, distributed denial-of-service (DDoS) attacks were making headlines, and now ransomware has come into heightened focus. It's reasonable to believe that other types of attacks will emerge in another two years and continue to change thereafter.

Yet even though cyber risk evolves, it's possible to understand what the financial implications of an attack might be by using what's known as a cyber risk quantification (CRQ) model. These models analyze past events to predict what the financial impacts of future cyber events might be.

But not just any model will do. Enterprises need insurance-validated risk models, meaning the model is strong enough and has both the breadth and depth of data to be trusted to quantify cyber risk across an insurer's large portfolio. Enterprises need this level of sophisticated models, which are continuously validated at scale, if they want to be prepared. Otherwise, they may be using a stagnant quantification method that limits their ability to account for their financial cyber exposure to current and future new threats.

Modeling the Unknown

Part of quantifying something dynamic like cyber risk means having a robust modeling framework. Using what's known as impact-based modeling allows for quantifying "known unknowns."

In other words, a modeling framework that can reflect new emerging threats and utilize risk models that tie together multiple areas of risk — for example, certain events affecting an enterprise, the severity of past attacks, the frequency of events, etc. — can come to a conclusion about the financial impact of future events.

Even if the specific type of attack remains unknown, enterprises can at least have a sense of what their exposure would look like by relying on impact-based modeling, which provides an estimation for potential financial losses that will be driven by cyber events.

Continuous Validation and Calibration

Over time, high-quality risk models become increasingly accurate due to continuous validation and calibration. As new cyber threats emerge, so too does a deeper understanding of event footprints, the technology or service provider involved, and the propagation pattern of the infection. While it's important for companies to be aware of evolving cyber threats and types of attacks from a risk management perspective, such as to educate employees and mitigate attacks, putting a financial quantification on cyber risk is the most efficient way to understand "how" the attack landscape can affect a specific company. A $1 million loss, for example, is still $1 million whether it came from ransomware or a DDoS attack. By focusing on an impact-based approach, the emphasis is still on quantifying the loss, rather than trying to predict exactly how cyber events may evolve.

A cyber risk quantification model can also be calibrated by looking at what the model projected and seeing how that aligns with events that actually occur over time. Doing so requires data at scale. If you only know the financial implications of events that occurred at, say, three companies, then that doesn't give much information to feed and calibrate the model. Yet if there are thousands of events to analyze, such as by looking across an insurer's entire portfolio, that provides a much better view into what's happening across the cyber risk landscape. From there, this data can be used to improve the model.

Breadth and Depth of Data Sources

As alluded to, a robust cyber risk quantification model requires data scale. Yet it's important to have both a significant breadth and depth of data sources. Doing so enables a model to understand what's happening across industries as well as what risk might look like in more specialized circumstances.

However, many cyber risk modeling vendors focus on specific areas, whether that's looking at industry risk, geographic risk, certain types of cyber attacks, etc. So, going both wide and deep requires pulling together a broad set of data sources and digesting huge amounts of data.

Having proprietary data makes a meaningful difference too. In addition to sifting through the data that is publicly available and data acquired through cybersecurity data partners, leveraging unique data collected by insurers as well as from enterprises can help set a model up for success.

Tapping Into a Data Flywheel

The beauty of Kovrr's platform is that it serves two types of entities: insurance carriers and enterprises. That provides a very unique flow of this aforementioned proprietary data. That can be used to train and bring cyber risk quantification models to a level of accuracy and precision that essentially can't be achieved otherwise.

Insurance carriers get the benefit of understanding financial risk based on what enterprises themselves report, which they would likely not provide in so much detail on their own to insurers. Enterprises are not obligated to provide this financial data to Kovrr, but many do opt in, and their anonymized data feeds the model to strengthen it for all.

Likewise, enterprises gain the advantage of tapping into data from insurance companies on the financial impacts of attacks that they or third-party vendors might not get on their own. As such, insurers and enterprises can benefit from a flywheel effect, where the data from insurers strengthens the risk models enterprises utilize, and the data from enterprises strengthens the risk models insurers utilize to assess their portfolios, which loops back to strengthening what enterprises know. Over time, sharing this data through Kovrr leads to continual improvement of cyber risk quantification.

Leverage the Power of Kovrr

As an enterprise risk management professional, if you want to be able to thoroughly quantify cyber risk, then it's important to use insurance-validated models. Kovrr has a robust modeling framework with a unique flywheel of data collection (from both insurers and enterprises) that continuously feeds improvements to the cyber risk quantification models. With Kovrr, enterprises gain the advantage of using risk models that are strong enough to be trusted by cyber insurers across their portfolios.

> Ready to get a solid handle on the financial implications of cyber risk, especially as new threats emerge?
>
> Get in touch with Kovrr today to see how we can help you be prepared.

KOVRR
Cyber Risk Modeling

The Author

Yakir Golan

CEO

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