KOVRR
Cyber Risk Modeling

www.kovrr.com

Renewing Cyber Insurance? Leverage CRQ To Assess Needed Coverage

JANUARY 2022

When you purchase auto insurance, both you and the insurer conduct an analysis of each other. The insurer checks out your driving history, the car model (what safety features it has) and where you store and drive your car. Meanwhile, you're deciding how much coverage to purchase. For example, do you really need a low excess, legal expenses cover and breakdown cover?

The same principles apply when you decide to purchase or renew your cyber insurance. But how do you know exactly how much risk to transfer? What are the best methods for effective quantitative analysis in cyber insurance investment decisions? You can either guess or base your decisions on actual data by utilizing Cyber Risk Quantification (CRQ).

What Does Cyber Insurance Cover?

Traditional commercial general liability and property insurance policy providers have started to specifically exclude cyber risks in their terms and to write back the elements that they intend to cover, in some cases none. For this reason, cybersecurity insurance has emerged as a stand alone line of coverage.

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption and network damage. The coverage provides protection against a wide range of cyber incident losses that businesses may suffer directly or cause to others, such as:

- Data destruction and/or theft
- Extortion / ransom demands
- Denial of service attacks (DDoS)
- Crisis management activity related to data breaches
- Legal claims for defamation, fraud and privacy violations
- Regulatory & privacy compliance penalties

Some of the more common cyber insurance claims are triggered by ransomware, fund-transfer fraud attacks and business email compromise scams.

The Two Sides of Cyber Threat Evaluation

Just like auto insurance, the vetting process considers two sides. On one hand, the car itself is evaluated. Does it have airbags, anti-lock brakes and evasive steering assistance? If it does, it's safer, and this may lower the insurance premium.

The same concept applies to business security. That is, how well protected are you against an attack? How well developed are your security Policies & Practices? How solid are your firewalls and encryption? Do you have a data backup solution for critical data and system configurations? Have you implemented multi factor authentication or identity access & management (IAM)? What does your software patching and update planning look like? How do you train your staff to ensure they are not the infiltration point?

It's critical to evaluate your security readiness when making decisions about buying cyber insurance. Only a clear picture of where you stand now enables you to make the right capital management decisions.

However, security readiness is only part of the equation. Accurately assessing whether a threat is real and potentially damaging is also critical. Are you going to buy flood insurance in the desert? Of course not. Likewise, having detailed data about current and emerging threats enables you to determine where you need more cyber insurance and where you need less. For some areas you might not need any insurance at all if your risk acceptance level falls below a certain threshold.

Cyber Insurance Decision Making Process

How can CFOs make informed decisions about cyber risk transfer and risk acceptance? In the past, financial cyber risk quantification was a long, painstaking process. Lengthy workshops, complicated questionnaires and interviews were the only way to reach a conclusion.

Even despite this rigor, any insight gained was not always based on quantifiable threat data. Also, once the evaluation process was completed, it immediately began to lose its validity. If there's one thing today's threat landscape has shown us is that nefarious tactics evolve rapidly in scope and sophistication.

As time goes on, a company's intrinsic security profile changes along with its relationship to the threat environment. So where do you get clear risk transfer insights?

Cyber Insurance & Cyber Risk Quantification

Insurance has always been heavily dependent on data, and insurance companies go to great lengths to collect and analyze data. This way they cultivate a viable insurance business model and provide a valuable service.

Cyber risk quantification (CRQ) aligns with this process by assessing cyber risk based on real world data. For example, Kovrr's CRQ provides access to global threat intelligence and financial impact data based on actual cyber incidents and cyber insurance claims. The data is presented in a clear, understandable manner, with associated risk vectors, damage types and other easy to access data.

Even better, Kovrr's CRQ provides the data on-demand. This means you have the ability to assess the risk at any time, and the data reflects the current risk scenario which evolves over time.

Cyber Risk Quantification (CRQ) Assesses the Financial Impact of Events

Rather than speaking in vague terms about cyber security, CRQ provides clear insight into your financial exposure to different types of events. The assessment takes into account your organization's security readiness, external threat actor activity and potential third party risk factors.

By applying CRQ, your organization can gain intelligence as illustrated by the chart below.

Clear Business Language Empowers Decision Making

It's not your IT team's job to make insurance and investment decisions, even when it comes to cyber security. For cyber insurance related capital management decisions, quantitative analysis usage in prioritizing risk is essential. The CFO needs to quickly grasp the data and its conclusions. Accurate and transparent information is critical for sound governance.

Kovrr bridges the gap between the complex world of cyber threats and boardroom decision making. With methods such as cyber risk modeling and cyber risk quantification, risk scenarios can be translated into understandable business terms. Outcomes can be improved as decisions are made based on large scale data in a consistent way. Plus, the data is available on-demand and updated to provide close to real time relevance.

Kovrr financially quantifies cyber risk on demand. Our technology enables decision makers to seamlessly drive actionable cyber risk management decisions. The Kovrr platform empowers Chief Risk Officers, CISOs, underwriters, exposure managers, risk professionals and catastrophe modelers to understand, financially quantify and manage cyber risk.

> **Get in touch** with Kovrr today to see how we can help you financially quantify cyber risk.

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