KOVRR
Cyber Risk Modeling

www.kovrr.com

What Is Cyber Risk Quantification (CRQ)?

JUNE 2021

Cyber Risk Quantification (CRQ) enables enterprises to assess and manage their cyber risk by putting cyber risk in clear business terms. In other words, organizations can understand how cyber risk specifically affects potential revenue, profit, and other measures of financial success.

Yet as important as cyber risk quantification is, enterprises often do not have a clear-cut data regarding the cyber risks they face. In many cases, the risks themselves are unclear, with organizations lacking the data needed to understand the frequency of the different types of attacks that exist, the severity of these attacks, and how these attacks leverage vulnerable technologies and third-party service providers which are specific to an organization's own digital footprint.

In this guide to cyber risk quantification, we'll look more closely at:

- What goes into cyber risk quantification
- How to conduct cyber risk quantification
- How to leverage cyber risk quantification

What Goes Into Cyber Risk Quantification?

When looking at cyber risk quantification, it's important to acknowledge that this term isn't just about assigning a general value to the cyber risk for a single enterprise or an insurance carrier's insured portfolio. Instead, cyber risk quantification is about analyzing data that enables organizations to get specific on how cyber risk affects them.

Yet before an organization gets too far into the cyber risk quantification process, it's important to first be able to define a cyber event and understand what happens when these events occur. Otherwise, it's impractical to assign a dollar value to cyber risk when it's unclear how different types of events might affect a business.

Understanding Cyber Events

In short, a cyber event is any occurrence where data is compromised based on the framework of confidentiality, availability and integrity — the so-called CIA triad. There could also be the fourth element of ransom, or potential for ransom. Thus, data doesn't necessarily need to be stolen, as a cyber event could involve the availability of data, causing business interruption, such as when a cyber attack prevents a company from accessing its data.

© 2021 Kovrr All Rights Reserved

The Golden Triangle of Cyber Risk Quantification

To more specifically understand the types of cyber events a company may face, and to therefore facilitate cyber risk quantification, organizations need to be able to pull together data in the following three areas, which can be considered the golden triangle of cyber risk quantification:

- **Cybersecurity resilience**

  Organizations need to understand their security posture to see how the frequency and severity of attacks may apply to that enterprise. In other words, organizations need to map their digital footprints from both the outside and inside, such as identifying which security controls they have in place and test their efficacy to understand where their vulnerabilities lie.

- **Frequency**

  Organizations need data on the frequency of cyber attacks, by analyzing past and ongoing cyber events globally, updated in as close to real-time as possible. What may seem like an infrequent type of event one day can quickly turn into a more frequent threat - organizations need data that enables them to keep up with how cyber risks evolve.

- **Severity**

  Organizations also need to understand the potential financial loss due to different cyber risks. Severity can be quantified based on:

  a. The intensity of an event, for example, how much data was affected or how much ransom was requested.

  b. The severity of the loss, for example, the cost of data recovery, losses accrued due to business interruption, forensics, etc.

Cyber Threat Intelligence

A cyber event can involve either one or both of the following:

- **Attacks leveraging vulnerable technology**

  A cyber event may affect on-premise technology, such as when a ransomware attack prevents a company from accessing files stored on a specific computer.

- **Attacks targeting third-party service providers**

  When companies use third-party providers, such as email service or cloud data storage, that could also create cyber risks. A cyber event affecting these service providers can cause business losses for not just the provider but their customers as well. However, these attacks tend to have a more defined timeframe, like natural catastrophes, which can make cyber risk quantification easier.

© 2021 Kovrr All Rights Reserved

Multi-Model Risk Analysis

Having the ability to differentiate between types of losses is important to understanding the types of events that could impact an organization and can be done using a multi-model approach. These different types of cyber events can then cause different types of losses, which can be broken down as follows:

- **Attritional losses**

  These losses are from events that tend to have a high frequency of occurrence but low severity in terms of financial damage.

- **Large losses**

  These losses might only affect one specific company due to a targeted attack and will lead to a substantial loss. These losses tend to have a low frequency of occurrence but high severity in terms of financial damage.

- **Catastrophic losses**

  These losses are from systemic events that tend to have a low frequency of occurrence but high, widespread severity in terms of financial damage.

As companies begin to understand the types of cyber events that may pose a risk to them and the losses that these events are typically associated with, they can then start their cyber risk quantification.

How to Conduct Cyber Risk Quantification

To specifically come up with a dollar value for cyber risk quantification, enterprises need to source and analyze the data from each side of the golden triangle of cyber risk quantification.

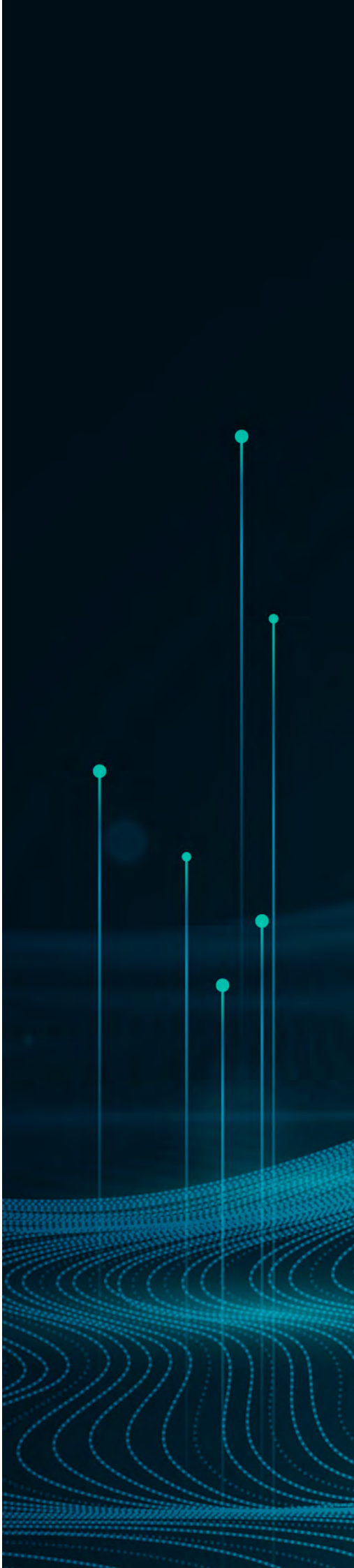
From there, companies need to bring all this information together to understand the types of cyber events they might face and how that may translate into monetary impact. This includes mapping the cost components of different events to understand the different types of financial impacts that may occur.

For example, a cyber event that causes business interruption can have expenses in areas such as public relations to minimize the reputational damage that can occur, as well as lost revenue from not being able to operate the business as usual during this period of interruption. Understanding these different cost drivers is necessary to gain a full understanding of a company's exposure, as well as to then determine a cost allocation per event by modeling the impact that a specific type of event is likely to have on an organization.

Using Impact-Based Modeling to Conduct Cyber Risk Quantification

Putting a specific exposure number on cyber risk requires modeling the impact of different cyber events. A company may know the types of events they could face, the severity of past personal events, the vulnerability of specific devices inside the organization, etc., but there still needs to be a way to pull everything together into a cohesive quantification, taking into consideration global attack frequency and severity of attacks.

© 2021 Kovrr All Rights Reserved



Enterprises need a risk model that measures financial value by:

- Assessing the impact from previous cyber events
- Analyzing hypothetical events that could happen to an organization based on historical events (looking at frequency and severity) in relation to an organization's security posture. Doing so helps specify "known unknown" events.
- Running a Monte Carlo simulation to assess losses in future years.
- Creating a yearly loss table that provides a specific financial loss amount for each event based on the information analyzed in the preceding steps.

Enterprises need to be able to model the potential magnitude of events and the likelihood they would suffer from them. To reflect this, we produce a probabilistic model using exceedance of probability curves to summarize the outcome of a monte-carlo simulation. The two types of exceedance curves include:

- **Occurrence Exceedance Probability (OEP)**

  Looking at the cyber event with the highest amount of damage in a given year allows for the assessment of the probability that one cyber event would have a maximum financial loss above a given amount.

- **Aggregate Exceedance Probability (AEP)**

  Summing the damages from cyber events over the course of a given year allows for the assessment of the probability that the aggregated financial loss from cyber events in a particular year exceeds a given amount.

How Can Organizations Leverage Cyber Risk Quantification?

Understanding what goes into cyber risk quantification and how the data comes together to put cyber risk in financial terms is a big step toward managing cyber risk more effectively. Still, knowing this background is only part of the equation. Enterprises still need to decide how to leverage cyber risk quantification.

Some of the considerations include:

Timing

Ideally, cyber risk quantification should be conducted on a quarterly basis at minimum. If cyber risk quantification is only calculated once a year, there is a possibility that new technologies and service providers will be unaccounted for in the calculation. Therefore, it's important to have systemized processes, including having a reliable way to collect and analyze the data for the golden triangle of cyber risk quantification.

© 2021 Kovrr All Rights Reserved

Who's Doing the Calculations?

Organizations essentially have three options to turn to in terms of who will do the calculating for cyber risk quantification:

- **Professional services firms**

  Consultants, accountants and other professional services firms may be able to provide a general calculation for cyber risk quantification but may lack sufficient cyber expertise, particularly as it pertains to data collection and modeling, so it's important to vet these firms accordingly. The timing can also be quite lengthy compared to other options.

- **Internal, subjective analysis**

  Companies may be able to rely on their own data and the subjective experiences of the company and individuals within given teams to quantify cyber risk. Yet this can be an imprecise method

- **Third-party cyber risk experts**

  Similar to professional services firms, but with a focus on cyber risk, third-party experts could be used to quantify cyber risk. Third-party experts, including Kovrr, have their own solutions, data sources and models, along with their internal knowledge of cyber risk quantification, to produce timely and accurate results.

Benefits of Cyber Risk Quantification

To leverage cyber risk quantification, organizations need to understand the benefits of these calculations. From there, they can then choose how to apply these insights to improve their businesses overall. Some of the benefits of cyber risk quantification include:

- Understanding exposure in different areas of a business or insurance portfolio so as to not exceed risk limits.
- Being able to budget for cyber risk appropriately, rather than being caught off guard by huge, unexpected expenses.
- Adhering to reporting requirements for boards, risk committees, shareholders, regulators, etc.
- Improving the use of capital, e.g., by enterprises being able to invest in a way that accounts for cyber risk. Insurance carriers can also obtain more appropriate reinsurance based on a precise understanding of the value they need to insure.

© 2021 Kovrr All Rights Reserved

KOVRR
Cyber Risk Modeling

While leveraging cyber risk quantification may seem a bit complicated for those unfamiliar with this area, it's very important for organizations to understand their risk and potential financial losses that can occur from cyber events.

Many organizations don't have any idea of how much risk they actually face and what that means in terms of monetary amounts that could be at stake. By using cyber risk quantification processes and tools that pull together data, both enterprises and insurance carriers can gain clear insights into their exposure and be more prepared for the financial impact of cyber events.

Ready to stop guessing and start getting real, actionable business insights when it comes to cyber risk?

Get in touch with Kovrr to learn how to simplify and benefit from cyber risk quantification.

© 2021 Kovrr All Rights Reserved

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

© 2021 Kovrr All Rights Reserved