KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

Elevating Cyber Risk Management to Enterprise Risk Management

MARCH 2022

For too long, cyber risk has remained outside the mainstream of Enterprise Risk Management (ERM). In reality, the risks facing a business from a cyberattack are not all that different from other risks, such as those arising out of operations, interest rates or toxic chemicals. Each type of risk has a likelihood of occurrence and a potential loss in the event of a problem, e.g., if a company does not handle toxic chemicals properly, there is a certain probability that it will experience an accident, which will then require money to remediate. A cyberattack is much the same.

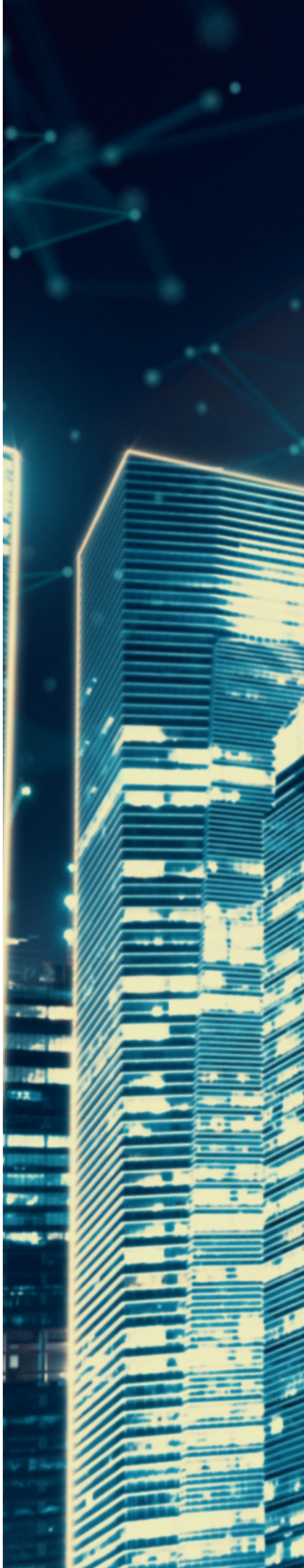
Unlike interest rates or toxins, however, cyber risk has been hard to quantify. Reasons for this included the highly technical nature of cybersecurity, which made it difficult for traditional ERM professionals to handle. Cyber is an esoteric field. It has been challenging to assign probabilities to different kinds of attacks and quantify their costs.

Cyber risk quantification (CRQ) is changing this status quo. CRQ makes it now possible to estimate the financial impact of different kinds of cyberattacks. With this new capability, cyber risk can be subject to standard financial quantification and risk management processes.

Understanding the financial impact of cyber events on your business

A cyberattack costs money. The expenses of dealing with an attack include the work of remediating the damage. The IT team may have to re-image infected devices or hire a consultant to apply software patches. There may be legal and public relations costs, as well. The process of informing customers of a breach can be quite costly. Brand damage should also be factored into the process of putting a monetary value to a cyber risk.

One thing to bear in mind, though, is that a cyber attack may not carry a high cost. Some will. Others will not. For example, a routine takeover of a production server might be addressed in an hour and cost effectively nothing to fix. A serious data breach, on the other hand, might cost millions of dollars to remediate. Each industry has its own risk cost characteristics, based on the value of their digital assets and attack surface area. A bank, for instance, might face higher costs for dealing with a cyberattack than a retailer.



Cyber risk and ERM

ERM professionals use specialized techniques and software to rate risks across a business. They will differentiate between inherent risks and residual risks in various categories of risk, such as treasury, compliance and IT. Residual risk refers to risk that cannot be mitigated through insurance or other countermeasures. The rating of a risk, which is based on metrics, may be high, significant, moderate or low. The higher the residual risk rating, the more costly and probable it is that the risk will turn into a loss.

An ERM dashboard might plot risks according to potential likelihood and financial impact on a "Risk Heat Map." Now, with CRQ available to produce meaningful cyber risk metrics, ERM teams can include cyber risk on their Risk Heat Maps. Kovrr's Quantum Cyber risk Quantification solution enables this capability. It can estimate low and high potential levels of cyber risk exposure and assign costs to those levels. It can break down cyber risk by category, too, showing the potential losses for risk drivers like ransomware, business interruption and so forth. Using this data, ERM teams can rate the level of residual risk based on the projected likelihood of losses and estimated financial impacts.

Working with the board of directors

If cyber risk can become part of the broader ERM process, it can be included in board-level conversations about risk management. The board, after all, is where important decisions get made about where to invest in risk mitigation. With CRQ, cyber risk is now part of the discussion. Board members can compare cyber risk with other forms of risk and make informed decisions about where cyber risk warrants an expenditure of funds.

CRQ can help the board prioritize cyber risk management decisions. Should the company invest in a SOC Should they make the move to a Secure Access Service Edge (SASE), which may require a substantial outlay of funds? By understanding the potential losses in the event of a cyberattack that targets a vulnerable area of the IT estate, the board can make decisions based on real data, not hunches.

To learn more about the KOVRR'S CRQ solution, contact us to book a demo.

The Author

Gil Hazaz

VP Sales, Enterprise Solution

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