KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

Top 3 Reasons Why You Need Cyber Risk Quantification

FEBRUARY 2022

One of the great ironies of enterprise technology is the tendency of its practitioners to extol its extraordinary digital accuracy while promoting its use with the vaguest of promises. A strategic investment in a new platform might be justified with a notion like “the cloud is the future.” Yes, but how much will that cloud future earn for the business?

Cybersecurity has the same problem. Decision makers demand financial indications, one holistic view and not dozens of different security measures, to evaluate the potential financial impact of cyber risk on their businesses. This is what cyber risk quantification (CRQ) is about. CRQ leverages data analytics to provide one holistic financial view powering wiser risk management decisions. With that in mind, here are the top three reasons you need to adopt cyber risk quantification to elevate your business cyber risk management decision making process to new heights.

01 Understand the Financial Impact of Cyber Events on Your Business

What is the financial impact of a cyber event on my business? The true answer may surprise you, either positively or negatively. Common types of cyberattacks may only cause minor financial damage. A phishing attack, for example, might require the re-installing of server software and wiping an end user’s laptop. That’s not going to cost a lot. A major data breach, on the other hand, could cost millions to remediate, once factors like legal liability, external consultant fees, duties of notification and public relations are considered.

Knowing the dollar value of your cyber risk is a starting point for making decisions about how much cyber insurance to buy and which specific coverages are relevant to your business. Once you can financially quantify your cyber risk, you will be well-informed when it comes to developing security policies and managing the cybersecurity function in your business.

02 Assess the ROI of Cybersecurity Investments

Businesses and public sector organizations are spending a great deal of money on cybersecurity. Estimates vary, but industry research pegs the global cybersecurity market at somewhere between $150 and $200 billion a year. It’s growing every year, with one research firm predicting that cyber spending will top $366 billion by 2028. There is no shortage of places to invest in cybersecurity. The most important question to answer, however, is what is the right place (and amount) to invest?

If you can put monetary value to your cyber risks, you can start to figure out your return on investment (ROI) for

cybersecurity solutions and services. It may not be possible to get to the nearest dollar, but you can definitely use CRQ to figure out if you are in the right ROI zone.

For example, let's say your CISO wants your board to approve a $5 million expenditure on a security operations center (SoC). Should the board approve the investment or not? In general, boards tend to be quite good at assessing investments in the context of risk. They routinely consider investments to mitigate credit risk, product liability risk, interest rate risk and so forth. With cybersecurity, however, boards and c-level executives can become frustrated because there's typically little data about financial payback.

If the SOC investment is $5 million, what's the risk worth? If a company is doing CRQ, the CISO is able to tell the board for example that the risk is valued at $10 million, so the SOC is a good investment. Alternatively, if the company's SOC implementation is worth $1 million potential risk reduction, then the CISO probably wouldn't even consider a SOC at such a large scale.

03 Prioritize Cyber Risk Management Decisions

Cyber risk quantification can facilitate cyber risk management decisions. Cyber risk management, and related spending, should correlate to potential financial impacts of risk exposure. For instance, if email security risks threaten a company with $1 million in losses, but phishing could cause $10 million, then phishing should probably receive priority for risk mitigation.

This is about more than just spending and ROI. CRQ lets security managers and other stakeholders determine which policies and countermeasures deserve the highest priority. For instance, a company might need to decide whether it wants to undertake a complex, time-consuming patching project or implement a new anti-malware email filter. They might only do one project at a time. CRQ can help them figure out which should come first.

Kovrr's Quantum Cyber Risk Quantification platform enables decision makers to understand and financially quantify the changing profile of their cyber risk exposure.

> To arrange a demo, visit https://www.kovrr.com/cyber-risk-quantification

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