KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

Managing Cyber Risk with Cyber Risk Quantification

APRIL 2022

Cybersecurity leaders are struggling with a simple question that tends to be difficult to answer with any accuracy: What is the cost of a cyber attack on our organization? Industry research, such as that provided by the respected Ponemon Institute, offers an average figure, which is around $4 million. However, that data point is not all that useful, in reality. Some cyber attacks cost effectively nothing. They're routine, resolved in the course of a day's work. Other attacks can be catastrophic, even threatening a company's survival.

So, what is the cost of a cyber attack? It's somewhere between zero dollars and kill-the-business. Senior business managers, boards of directors, insurance carriers and other stakeholders all need a more precise answer. To address this need, businesses are adopting a process known as cyber risk quantification (CRQ). The goal of cyber risk quantification is to develop an accurate estimate of the costs of cyber risk exposure. The CRQ process involves multiple streams of analysis that incorporate company-specific cost models with loss data from industry peers and other factors.

Why the Experts all Agree That Quantifying Cyber Risks is a Necessity

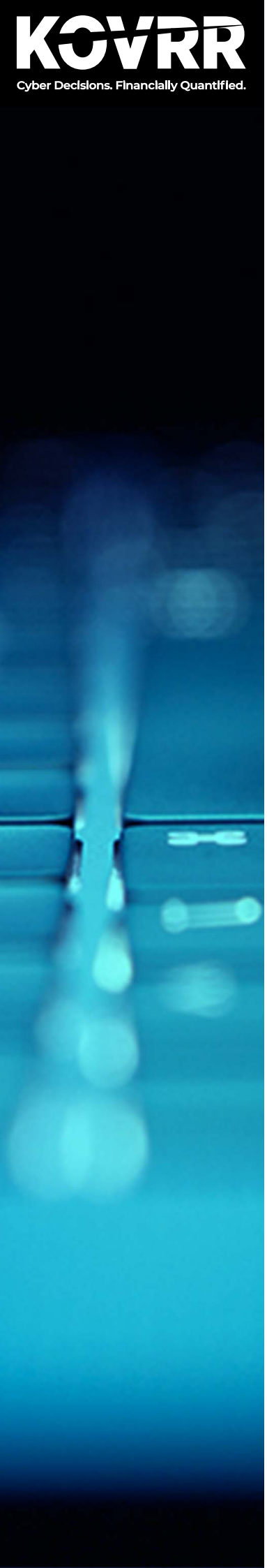
Quantifying cyber risks is a necessity today because most businesses are caught in the grip of powerful digital forces that promise great value, but also threaten serious losses if not well contained. On the positive side, the world is experiencing an accelerating process of digitalization. This trend has tremendous upside. At the same time, as businesses go digital, they are exposed to an increasingly potent cyber threat landscape.

The stakes are huge. Quantifying the financial risks of different cyber threats enables decision-makers to understand and financially quantify the changing profile of their cyber risk exposure. Management can think about cyber risk in practical terms. The process enables them to understand the business aspects of cyber risks and make informed decisions.

The race to digitize business

Businesses worldwide are embracing digital transformation. Research by Accenture reveals that 100% of businesses rely on the Internet for their operations. In this context, Gartner research found that 91% of companies are engaged in a digital initiative of some kind. Eighty seven percent of senior executives are making digitalization a priority.

KOVRR
Cyber Decisions. Financially Quantified.



The overhanging cyber threat

Digitalization comes with downside risks. Not only are complex digital assets challenging to manage, they are also vulnerable to attack. The last few years have certainly shown the devastating financial impact of major cyber attacks. Highlights include the WannaCry ransomware attack that cost the UK National Health Service over $100 million to remediate, to name just one of many victims. The Equifax breach cost that company over $4 billion to deal with, and notpetya resulted in a loss of $1.3 billion for Merck, the pharmaceutical giant.

Difficulties translating cyber risk into business risk

Given this threat environment, it should not be surprising that 68% of business leaders believe their cyber risk exposure is increasing. When it comes time to analyze the risk, or make decisions about cyber defense, however, stakeholders often find themselves having difficulty translating cyber risk into business risk. Businesses and their management teams understand risk very well. What's been hard is to place cyber risk into that familiar format.

Reasons for this include:

- A tendency to discuss cyber risk in technical, not business management terms. It's "we need to patch 100 servers," versus the more meaningful, "we'll lose a full week of operations if we cannot correct this defect in our computer systems."
- Cyber threats are constantly evolving. It can be challenging for IT management and business management teams to keep up with the latest drivers of risk exposure.
- Estimates of potential losses are overly broad and not fact-based.

The need to quantify cyber risks

Out of this comes a compelling need to quantify cyber risks. The future of the business depends on digitization. The threats are extreme. Discussing the risks has proven to be difficult, given the tendency for stakeholders from IT, security and business management to speak in different languages. The language of money, however, is universal. Business management executives understand risk in terms of money. If it is possible to quantify cyber risk in financial terms, then a productive dialogue becomes possible Cyber risk quantification means knowing, with some degree of precision, the potential cost of residual risk in cyber. Residual risk refers to the risk exposure that exists after other mitigating factors have been considered. For example, cyber insurance might cover a certain amount of financial losses associated with a data breach.

The residual risk whatever amount of money is required to remediate the breach after the insurance has paid the claim. And, with cyber, there is always going to be residual risk. In a data breach, for example, there will be costs related to legal work and public relations, notification processes and so forth. Insurance will not likely cover all of these.

The cyber risk quantification process also looks at all major areas of cyber risk exposure. A company might have risks related to ransomware, email-borne threats, compromised endpoints, data exfiltration, compliance issues like GDPR, damage to IT assets and more. Each area of risk has its own unique cost profile.

The Key Benefits of Cyber Risk Quantification

The ability to achieve accurate cyber risk quantification delivers many benefits. The practice enables all relevant stakeholders to know their residual risk, in terms of cybersecurity. Cyber risk quantification gives IT, security and business management a common commercial language they can use to discuss where and how to spend on cyber. With estimated residual risk costs in mind for different sectors of the IT estate, it becomes possible to make risk management decisions with confidence and consistency.

For example:

- Engage with cyber insurance carriers in order to determine the right level of cyber coverage. A company that quantifies its cover risk does not have to deal with the consequences of being under- or over-insured for cyber attacks.
- Make the right kind—and level—of cybersecurity investments. Where should a company spend on cyber defense? Without quantification of risk, management's investment decisions will be based on guesswork and general industry research. With cyber risk quantification, stakeholders from security, IT and the business management can invest in areas where they face the most potential losses.

Having a sense of the cost of cyber losses can also affect preparation and incident response. For instance, what if an attack on the email server is understood to be a minor inconvenience, not a serious problem? If it can be easily and cheaply remediated, then the incident response plan can be scoped accordingly.

Cyber risk quantification enables security and IT managers to know what they are talking about when asked about the risks facing the business. This is always a good look. They can speak to the specific areas of risk and the costs of remediating a cyber incident in each area. Going further, cyber risk quantification allows for a more informed assessment of cybersecurity programs and the progress of various initiatives.

KOVRR
Cyber Decisions. Financially Quantified.

The State of Cyber Risk Quantification in Today's Environment

Cyber risk quantification is practiced inconsistently. The 2019 Ponemon breach survey revealed that fewer than half of respondents say they measure the costs of cyber risks. Just 41% of respondents try to quantify the actual damage. So, it would seem there is plenty of room for improvement in the quantification of cyber risk.

How to Manage Cyber Risks and Cyber Spend More Efficiently

Putting cyber risk quantification into action is not a push button process, but it is not a monumental challenge, either. Each company will have to do it their own way. In general, though, following steps are helpful in getting to a meaningful outcome.

Assessing the impact from previous cyber events

The place to start is with the cost of earlier cyber attacks. What was spent on remediation? The best practice here is to break out costs by category, such as IT, external consultants, legal, public relations and customer interactions. Fines and penalties may be relevant here as well. It's worth doing as much as possible to pin down specific financial outlays. Then, move on to intangible cost.

Create a "loss grid"

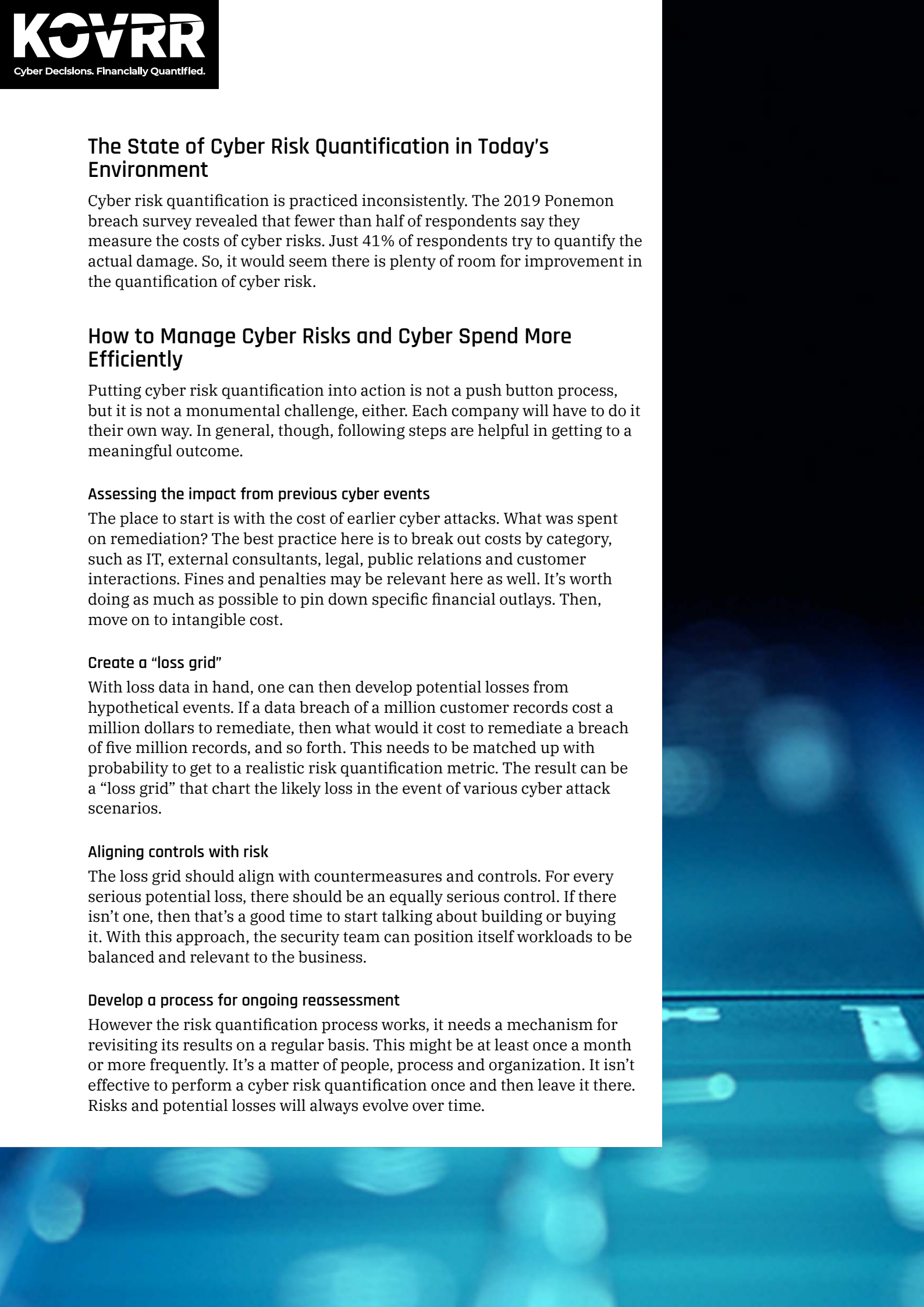
With loss data in hand, one can then develop potential losses from hypothetical events. If a data breach of a million customer records cost a million dollars to remediate, then what would it cost to remediate a breach of five million records, and so forth. This needs to be matched up with probability to get to a realistic risk quantification metric. The result can be a "loss grid" that chart the likely loss in the event of various cyber attack scenarios.

Aligning controls with risk

The loss grid should align with countermeasures and controls. For every serious potential loss, there should be an equally serious control. If there isn't one, then that's a good time to start talking about building or buying it. With this approach, the security team can position itself workloads to be balanced and relevant to the business.

Develop a process for ongoing reassessment

However the risk quantification process works, it needs a mechanism for revisiting its results on a regular basis. This might be at least once a month or more frequently. It's a matter of people, process and organization. It isn't effective to perform a cyber risk quantification once and then leave it there. Risks and potential losses will always evolve over time.



KOVRR
Cyber Decisions. Financially Quantified.

How Kovrr is Financially Quantifying Cyber Risk?

Kovrr offers on demand financial cyber risk quantification insights. The Kovrr Quantum solution leverages global threat intelligence and financial impact data from cyber incidents to quantify cyber risk. Users can drill down into examples of cyber events, along with associated risk vectors and damage types. Quantum is able to differentiate between systemic or targeted attacks and failures. It covers hundreds of thousands of simulated cyber events to generate accurate quantification metrics.

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