KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

Factoring Cyber Risk into Mergers & Acquisitions

JUNE 2022

KOVRR
Cyber Decisions. Financially Quantified.

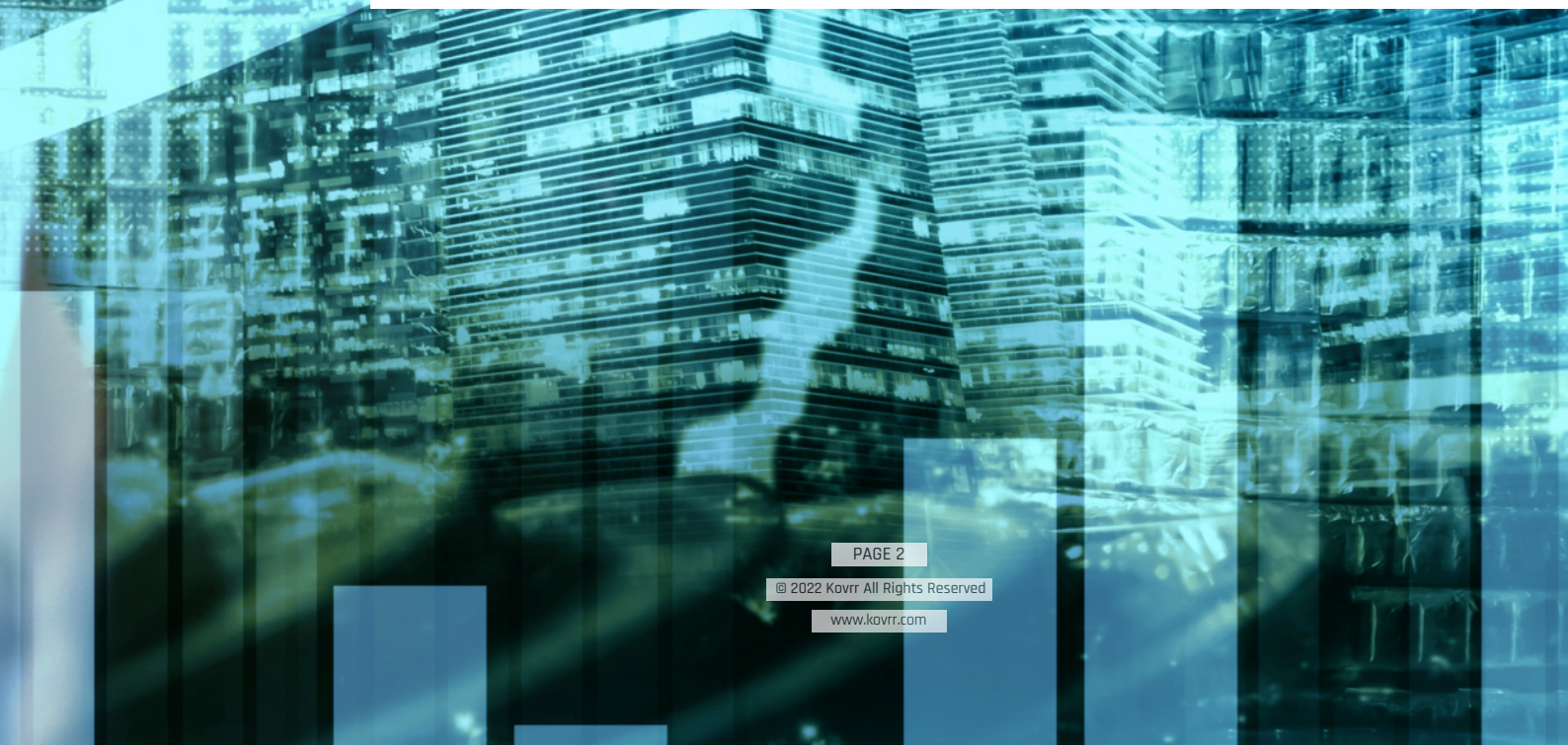
The merger and acquisition (M&A) process includes many elements, from valuations and due diligence to finalizing the deal itself. At each step, the acquiring entity carefully examines the acquisition target for risk, including credit risk, compliance risk, environmental risk and so forth. A serious enough unpremeditated risk, such as a pollution spill that will be costly to clean up, can affect the valuation, or even cause the entire deal to fall apart.

Today, cyber risk is beginning to be part of the M&A risk assessment process. Getting a firm understanding of the potential financial impact of cyber risk has traditionally been difficult, but that is starting to change with the development of cyber risk quantification techniques and tools.

Where does cyber risk fit into M&A?

Cyber risk is, or at least should be, a factor in M&A. For example, if the due diligence process uncovers an undisclosed data breach, then the costs of remediating that breach and paying regulatory penalties should affect the valuation of the entity. If the breach will cost a million dollars to fix, that million dollars should be deducted from the price the acquirer is willing to pay. If disclosure of the breach will negatively affect the reputation of the target company, then the resulting loss of brand value should also be reflected in the purchase price.

Potential cyber risk is equally relevant. An acquisition target that is exposed to significant cyber risk may become a costly company to own. If the acquiring company suspects that it may face millions of dollars in potential losses in the event of a cyber attack on the target, those losses could become a negotiating point in the deal. On a related front, if the target is determined to have deficient cybersecurity controls, then remediating those deficiencies may become a condition of closing the deal.



Challenges in understanding the true impact of cyber in M&A transactions

Despite the well understood potential for high cyber costs in an M&A transaction, cyber risks have not traditionally played a major role in M&A. The reason for this is that cyber risks have always been difficult to quantify. For instance, if due diligence shows that a target's servers are not patched, it is possible to put a price tag on performing the needed patching. However, attaching a dollar value to the risk of those unpatched servers was a matter of guesswork. As a result, if the target company didn't patch its servers for a year after the M&A deal closed, the acquiring company would blindly bear that cyber risk. They would not know what it might cost them if a breach occurred because of the lack of patching.

Solving the problem by quantifying cyber risk in an acquisition target

If stakeholders in an M&A transaction can determine the costs of cyber risk, they can factor those costs into the deal, hence the need for cyber risk quantification. Cyber risk quantification uses advanced modeling techniques to analyze cyber risk data and other related information to estimate the financial impacts of cyber events. The process looks at losses from comparable cyber attacks at similar firms. The data for this analysis may come from cyber insurance claims. In the example of unpatched servers, cyber risk quantification could give the acquiring company a relatively accurate estimate of the potential costs of a security incident stemming from the deficiency in patching.

Cyber risk quantification helps the M&A process in several ways. In addition to establishing costs for cyber risks in the target company, it enables stakeholders to figure out a priority of concern and remediation. People who have gone through M&A deals will appreciate how this changes the dialogue between acquirer and target. It will no longer be driven by vague statements like, "You have a lot of cyber risks. We need you to drop your valuation by a million dollars." Instead, the conversation can be, "We have identified five areas of risk, ranging in value from $10,000 to $100,000. We insist that you remediate the $100,000 risk as a condition of this deal closing."

Cyber risk quantification can also help facilitate the post-merger "venture integration" phase of the M&A process. During this period, both companies get to work stitching the two organizations together. Departments merge, systems get integrated and so forth. IT department mergers and systemic integration are long, complicated and expensive processes. If the people responsible for doing this work have a well-reasoned and prioritized list of cyber risks to address, the process will yield better results—and result in less costly cyber risk exposure.

Kovrr and cyber risk quantification for M&A

Kovrr Quantum provides M&A teams with a solution for quantifying cyber risk. Quantum leverages global threat intelligence and financial impact data from cyber incidents. It gives M&A stakeholders the ability to drill down into cyber event examples, examining risk vectors associated with attacks that are common in the target's industry, along with industry-specific types of damage and other relevant data.

Want to see how Kovrr can help your company financially quantify cyber risk? Book a demo with our experts today.

The Author

Gil Hazaz

VP Global Sales

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