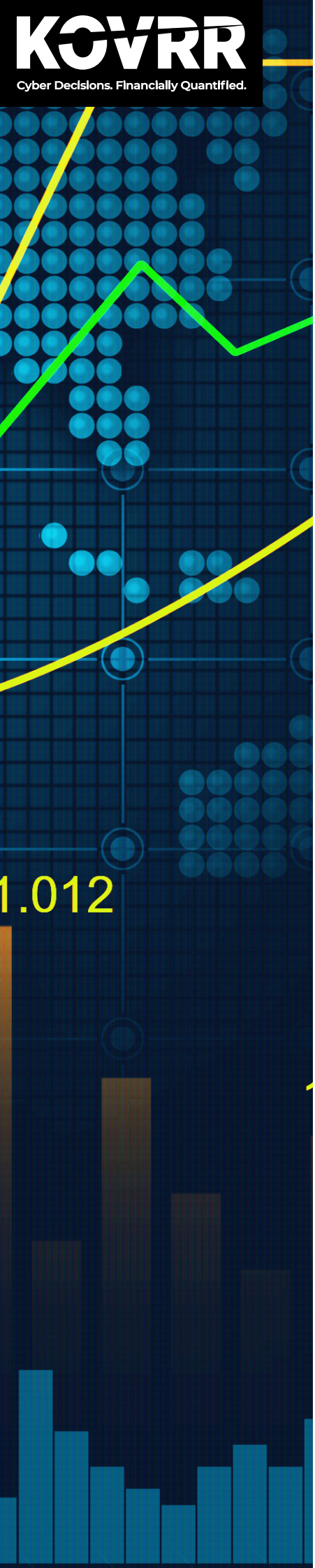
KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

Cyber Risk Quantification for Financial Services Organizations

MAY 2022



Building a Framework for Quantifying Cyber Risk for Financial Services Organizations

It should not be a big surprise to anyone that financial institutions are among the most common targets for cyberattacks. Not only do they hold financial assets that attackers might want to steal, they also represent a powerful economic force (and symbol) that some want to disrupt. For these reasons, according to research from IBM, 23% of all cyber attacks are directed at financial institutions. The problem is growing worse, too. Since the start of the pandemic, cyberattacks on banks have shot up by 238%.

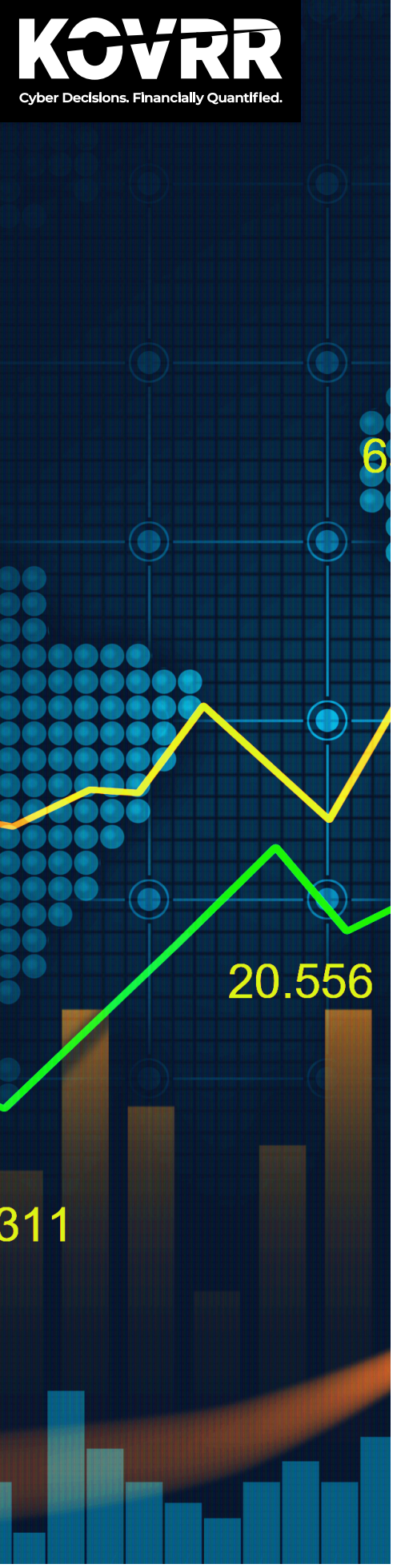
It should also not come as a great surprise that financial services organizations invest heavily in cybersecurity, and are generally quite good at it. The pressure is on, however, and getting more intense. As a result, financial institutions need to be getting better at cybersecurity all the time. Achieving this goal means understanding where to focus resources and where the status quo will be sufficient to protect digital assets.

Where to invest? That's always the big question. Cyber risk quantification (CRQ) offers a way to answer it. Cyber risk quantification gives financial services firms the ability to model cyber risks in financial terms—enabling them to make informed decisions about where to allocate limited cybersecurity resources.

Using Advanced Modeling Techniques Calculate for Modern Variables

Cyber risk quantification involves the use of advanced modeling techniques. The process analyzes cyber risk data, along with information about financial losses that have arisen due to cyberattacks. This data may come from cyber insurance claims from other financial services firms. It's a multi-model approach that differentiates between systemic or targeted attacks and failures. The process then further analyzes these data streams, evaluating them in the contexts of real world global cyber event frequencies, their financial impact and the company's firmographic and technographic profiles. After covering hundreds of thousands of simulated cyber events, the multi-model technique arrives at accurate risk quantification metrics.

KOVRR
Cyber Decisions. Financially Quantified.



Quantitative Financial Approach to Cybersecurity Risk Management

Cyber risk quantification estimates the financial impacts of cyber events. The process can thus drive effective risk management strategies. Consider the following risk management dilemma. An enterprise risk management (ERM) professional is confronting two different risks: 1) A ransomware attack that encrypts customer trading accounts vs. 2) A phishing attack that leads to account takeovers.

To determine the optimal allocation of resources, the ERM pro needs to understand the likelihood and impact of each risk. The problem is that too often, ERM people have to make decisions based on vague and subjective parameters like high/medium/low when it comes to the probability of an event and its impact. The ransomware attack might be assessed as medium probability/high impact, while the account takeover attack might be low probability/medium impact.

With that assessment, it makes sense to focus on the ransomware attack. However, these are guesses based on experience. It's better than nothing, but it would be much more helpful if the ERM professional could say, with some confidence, that the ransomware attack would cost the firm $500,000 to remediate, while the account takeover attack would cost $200,000.

How Quantification Addresses Challenges in Predicting the Evolving the Cyber Landscape

Done right, the cyber risk quantification modeling process is dynamic. It can be adapted to new threats and patterns. The process is able to address challenges in predicting what's coming next in the evolving cyber landscape. For example, ransomware is currently the number one threat, but that may not last. A year from now, some kind of supply chain attack might pose a more serious threat. ERM people can now model those future risks and come up with financial metrics to judge how seriously to take them.

Why Every Financial Organization Should Embrace Cyber Risk Quantification

Financial organizations should embrace cyber risk quantification for a number of compelling reasons. For one thing, the practice should lead to an improved overall security posture. It will also help manage residual risk, meaning risk that is not covered by insurance. Cyber risk quantification also gives diverse stakeholders a common frame of reference—money—for discussing complex, highly technical issues.

Business managers, IT managers and security managers tend to speak

different languages, which can lead to poor decision making and missed opportunities to improve security. When everyone can refer to a financial figure associated with a cyber risk, they can talk about it in a mutually meaningful way. It's no longer about "patch testing for Ubuntu Linux" but rather "we can avoid wasting a million dollars."

The metrics give decision makers from different disciplines the opportunity to focus their efforts on improving cybersecurity programs and controls. That way, they can have the biggest impact on risk reduction and risk exposure. Cyber risk quantification metrics also provide stakeholders with granular insights about the kinds of cyber events that might lead to extreme financial losses.

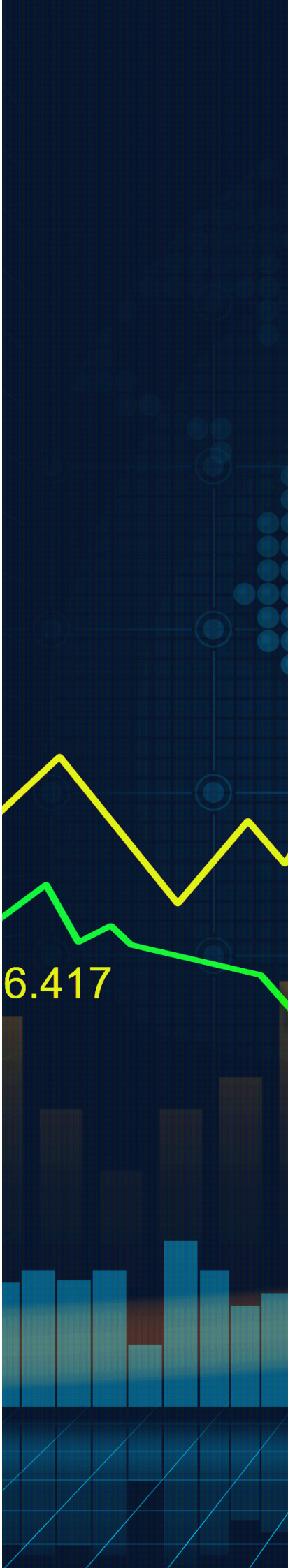
How Financial Services Organizations Build Trust Through Cyber Risk Quantification

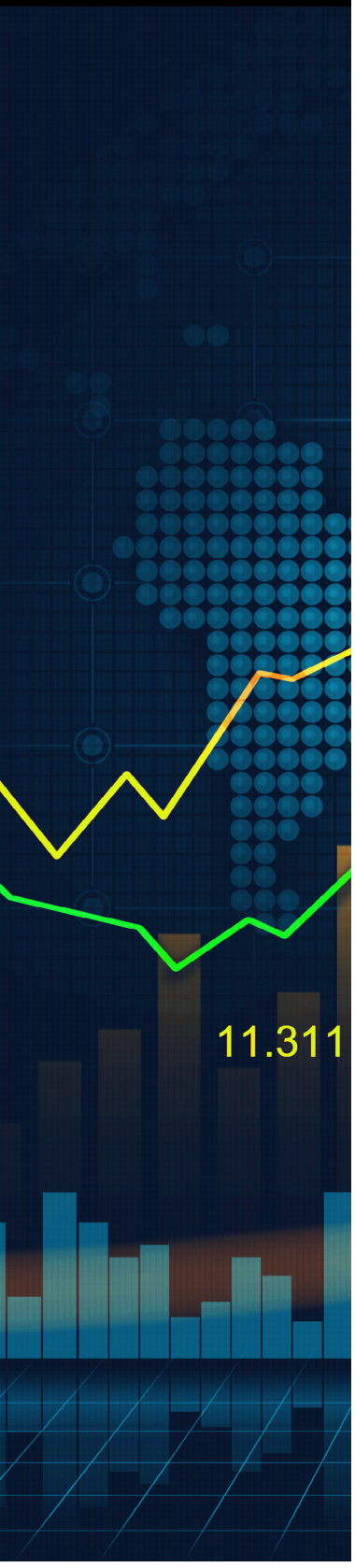
The financial services business involves many partnerships between firms. A banking app, for example, might connect with external stock trading firms' systems, insurance carriers and more. Investment banking transactions such as mergers and acquisitions require secrecy between parties, with severe consequences for breakdowns in confidentiality. For these reasons, it is critical that financial services firms establish strong trust relationships at the systemic level. Regulatory compliance, which often arises from security policies and controls, e.g., for identity management and encryption, is also essential for maintaining a firm's position as a trusted entity.

Cyber risk quantification does not prevent cyberattacks. Nor does it ensure compliance. However, by helping the business, IT and security leaders come together to focus attention and resources on the most pressing cyber risks, cyber risk quantification reduces the likelihood of a major cyber incident that can cause reputational damage and affect trust in the firm.

How Kovrr is Financially Quantifying Cyber Risk

Kovrr provides financial services firms with a solution, Kovrr Quantum, for quantifying cyber risk. Quantum leverages global threat intelligence and financial impact data from cyber incidents. It gives ERM professionals at financial services firms the ability to drill down into cyber event examples. It can examine risk vectors associated with attacks





that are common in the financial industry, along with industry-specific types of damage and other relevant data.

Quantum utilizes a range of modeling technologies, thus enabling users to differentiate between systemic or targeted attacks and failures. Users can enact simulated scenarios, tuned to the financial industry, to understand where their cyber security risks are concentrated. Quantum offers details of an attack scenario's financial impact on a financial services business.

Using Quantum, ERM professionals at a financial services firm can efficiently identify underlying issues that drive financial exposure from cyber threats. Quantum gives stakeholders from business, IT and cybersecurity the ability to assess the return on investment (ROI) for cybersecurity investments—along with metrics that can steer the prioritization of cyber risk management decisions.

Unlike traditional consulting engagements involving heavy investments of time and money, Quantum is an on-demand solution. It leverages global threat intelligence, filtered for relevance in financial services, coupled with financial impact data from cyber incidents. Users can drill down into cyber event examples, including associated risk vectors, damage types, and other relevant data. Security and risk management leaders at financial services firms can use Quantum to discover the underlying causes of financial exposure in cyber risks.

> 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