KOVRR
Cyber Risk Modeling

Hey CISO
Budgeting Season Is On

It's that time of the year... when budgets for next year are being prepared. Long sessions on what, when, and especially how much?

What's your view on the best way to do that? One way is to follow a practice that takes a fixed % of the IT budget. Other ways may include a pre-defined increase from the previous fiscal year. But at the end of the day, the real challenge is how do you gaze at the risk, quantify it and budget accordingly? How do you easily get a $ number you can stand behind and easily justify?

The problem with the status quo

So, here you are, in a tight spot. On the one hand you're expected to protect the business, its people, its data and to create value for the business, and on the other hand, you're expected to cut unnecessary budgets.

✻ Note to self - it doesn't matter how it wasn't really your idea to cut the cyber security budget, but if something goes wrong, you're still probably going to be the one who takes the fall.

The Paradox

There is an embedded paradox here:

Last year, you knocked on your CFO's door, asking for a budget in order to prevent something bad from happening to your company.

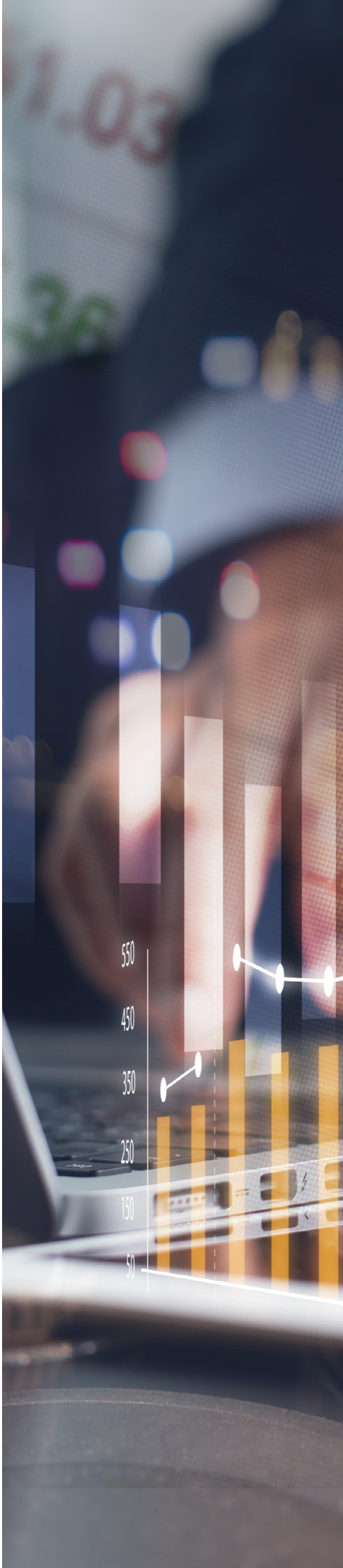
The year goes by, and it's time to knock on that door again. But now, the CFO says "we've invested millions last year, because you told the board bad things are going to happen, and that we should start putting money in, but nothing major really happened..."

Frustrated, you might be asking yourself - How do you mitigate this self-fulfilling prophecy effect? How sure are we that the risk we're mitigating is worth the millions we are spending?

Now what?

Well, maybe it's time, that in 2021 you'll have a way to base the conversation you're having with your board on real quantifiable $ numbers and on risk, vs. feeling perception, intuition CVE's, hype cycles and trends.

True, you have tried everything with your board - from security rating levels to red, yellow green, and high mid low. They get it. but do they really?



While going through the budgeting exercise, remember your target audience does not care about vulnerabilities and controls. They care about one thing, with regards to cyber risk: What is the financial exposure we have? What would the impact be if (when) something bad happens.

From that $ value of risk:

- How much should we allocate in risk mitigation (new/better controls)?
- How much should we allocate in risk transfer (Cyber Insurance)?
- How much are we willing to retain and take the risk?

The Solution

Give your audience what they need. Put the $ value on it, and help your organization take data driven decisions on cyber risk.

The challenges, risk wise, you're going to face in 2022 can be pre-modeled in a very scientific granular manner. Just like risk quantification is done for natural catastrophes such as; earthquakes and hurricanes, we apply similar methodologies to come up with the potential magnitude of losses from cyber incidents.

Combined with proprietary large scale data sets used to slice and dice it to model a bespoke risk quantification analysis tailored to your organization and business entities, on demand.

Why?

Because it's time to change the conversation with the board, and focus on risk and numbers.

To do that, **your source of Cyber Risk Quantification** modeling should understand all about frequency, probability and hold enormous scales of AI processed data to support it.

On a global level, Insurers have been and are continuously getting numerous claims stemming from a wide range of attacks, ranging from ransomware to you name it

Why now?

Because you need to justify your budget for next year, and you want to do It right.

Just imagine how much of that real-life, real-incident data is being accumulated with cyber risk insurers. Make sure your source of risk quantification modeling is drinking from these super valid and relevant springs. Sure, there are long, expensive, traditional analog ways to go at it, but is that fair?

To learn more about how Kovrr's modeling technology can quickly help you put a number on your financial exposure, before getting too deep into budget conversations, **get in touch today**.