How boards can quantify cyber risks: A primer for boards

*Chaitanya Kunthe & Gautam Sashittal

In our previous article, we spoke of the imperative of getting cyber risks and cybersecurity onto board agendas. We asked several questions that boards can ponder on, to start the process. This article focuses on whether cyber risks can be quantified, and if so, how?

Boards routinely assess and quantify risks as part of their ongoing ERM processes. But is this same rigour applied to quantifying cyber risks? Boards are often informed that cyber risks are difficult, if not impossible, to quantify. Problems cited range from the inability to identify the value of information to lack of quality data on cyber risks. Some of these concerns are indeed justified:

- How do you assign monetary value to the organisation's information?
- How do you quantify reputation loss should a cyber breach occur?
- Is there past data to reliably quantify cyber risks?

There are no easy answers to these questions. That being said, the challenges of quantifying these risks are not insurmountable. The answers lie in CRQ (cyber risk quantification); part science, but also part art!

What is Cyber Risk Quantification (CRQ)?

When you look at most people's "to-do" lists, all you see is an incomplete list of unclear stuff. – David Allen

Cyber-mature organisations maintain a risk register that lists all perceived risks to the organisation. Most risk registers, like most to-do lists, are an incomplete list of unclear risks and often unhelpful in supporting decision making in boardrooms. Risks range from 'so-obvious-that-they-are-silly', to the 'absurd'. For example, a common risk across most risk registers is the risk of a virus attack caused by a lack of antivirus software, the mitigant being an already installed antivirus! This clearly, should not feature in boardroom discussion!

By contrast, CRQ is the process of defining, clarifying and quantifying the organisation's cyber risks on two dimensions, the probability of occurrence, and the expected associated losses. A well-defined CRQ process enables boards to identify the organisation's risk appetite and take informed decisions.

Flawed approach to cyber risks

Cyber risks usually feature on board agendas for two reasons. First, nervous board members bring newspaper clips of recent data breaches and ask, "Can this happen to us?". Second, the IT team brings those same newspaper clips of recent data breaches to the board to request funding to implement a shiny new cybersecurity product or service.

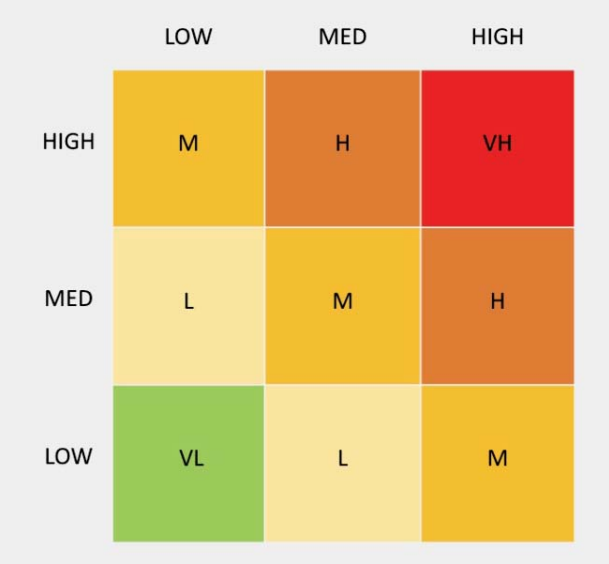
Asking about the possibility of a cyber breach is only half the story. Identifying the potential of a breach without quantifying the impact is like asking for the mileage offered by a car without knowing how much you would travel in a year. Useful information, but not actionable without the other piece – impact. And impact assessment can only come from the management and the board.

Cybersecurity team members highlighting piecemeal risks and requesting funding is why boards often avoid discussing cyber risks. It brings fear, uncertainty and doubt (FUD), without concomitant clarity. It is time for boards to change that, to take charge and be proactive rather than reactive.

Reimagining cyber risks

Boards are used to seeing risk heat maps. While visually pleasing, these charts offer little value in decision making.

If the risk of a ransomware attack is 'Moderate', what decision can the board take? Should the board approve the year-long project of upgrading the antivirus to an (endpoint detection and response) EDR tool? Will the EDR tool reduce the risk from medium to low? What does a risk reduction from medium to low mean? If the board approves budgets to reduce two medium risks to low risks, is it better than approving the budgets for reducing one high to a medium?



In our previous article, we listed some questions that boards should ask of their cybersecurity teams:

- What are our top 5 cybersecurity risks?
- What are our losses if they materialise?
- What are the chances of the risks materialising?
- How do we know if these are the top 5?

Trying to answer these questions naturally leads to Cyber Risk Quantification.

When must boards step in?

Boards must not leave implementation of a well thought-out CRQ programme to the cyber security team. The crux of CRQ, like any other risk management approach, lies in defining the right risk appetite. Boards should participate in workshops that clarify what 'risk' means to their organisation and assess their risk appetite. Professionally conducted workshops help clarify cyber risks.

Boards are uniquely positioned to brainstorm and identify the top risks to the organisation. For example, what may start off as a vague and general threat of 'ransomware attack' could be clarified as 'core banking system unavailability' – a key concern as it can lead directly to operational failure and regulatory fines. As the board brainstorms, clarity emerges. For example, operational impact and regulatory impact may be major concerns for this organisation.

Boards should also step in to clarify risk appetite. Can the organisation accept a US$ 5 million regulatory fine that occurs once in five years? Each impact area, ranging from reputational impact to financial impact can and should be clarified. Is a reputational impact where 10% of existing business is lost, or 5% of the market cap is placed at risk acceptable?

Data obtained from these workshops will aid the cybersecurity team in conducting CRQ assessments and provide the right data for boards to take decisions.

The CRQ process

The process of cyber risk quantification entails identifying risks to the organisation based on risk areas and appetites identified by the board in their workshops.

There are multiple approaches that cybersecurity professionals take for CRQ. To identify risks, standard approaches ranging from crown jewel analysis to business process analysis are adopted. Risks identified are then quantified using available past data, calibrated expert intuition and other statistical techniques to arrive at cyber risks for the organisation.

Boards should then expect data such as this:

"There is a 5% chance that a cyberattack on our core banking system can lead to a US$ 3 million revenue loss this year. Implementing a Web Application Firewall can reduce the chance to 2%."

The decision on allocating budgets can then be made based on these quantified risks.

No longer reading tea leaves

A properly implemented CRQ system moves cyber risk management from the realm of the occult to a scientific data driven system that is repeatable. The benefits of this in terms of clarity and direction for the organisation are well worth the time spent by the board in cyber risk quantification workshops.

In summary, CRQ is not rocket science. It is about asking the right questions and getting the right answers. It is about estimating financial impact if the identified risk events occur, even if that means taking a conservative view on the potential impact. It is about agreeing on the organisation's appetite to treat the risks that can be treated, and to accept the risks that

cannot be treated. It is also about assessing and creating the bench-strength within the organisation to manage these risks.

As we said earlier, CRQ is part science, part art!

*__Mr. Chaitanya Kunthe__ *is the COO of Risk Quotient, respon - sible for building and growing their cybersecurity consulting practice. He is also a consulting CISO to various organizations. He is a certified CISSP, CISA, ISO 27001 and ISO 22301 LA.*

*__Mr. Gautam Sashittal__ *is a Director at Risk Quotient. He has worked across diverse sectors and prior to to this was the CEO of the DMCC. A large part of his career prior to that was with the Royal Dutch Shell Group. He also serves as non-executive director on boards with focus on oil trading, hedge funds and trade finance.*