Deloitte.

Cyber Risk Quantification - A pragmatic approach

November 2023

Introduction

Traditionally, the way most organisations assess and rank risk (high, medium, and low) has been based on occurrence and severity, which is subjective, ambiguous, and qualitative. This method hinders timely decision-making and ultimately, business growth. As a result, organisations are moving towards more quantitative models of assessing risk that help them visualise the tradeoff between acceptable risk values and the business value.

Business leaders can take a more informed decision only if they are able to grasp the quantified risk value associated with a given opportunity. This will help them map the opportunity to the organisation's risk appetite, based on the threshold value of the risk.

Cyber Risk Quantification (CRQ), by definition, is a method to express risk exposure for an organisation in business-relevant terms. "Exposure" can be described in various ways including but not limited to currency value due to disruption to products and services, market shares, and customer retention during a given period. CRQ helps business leaders and the board understand the impact of cyber risk and becomes a driver to those informed decisions. CRQ is an imperative for organisations as it provides answers to some pertinent questions, such as:

- Are we investing enough or right to cater to specific cyber threats faced by my organisation?
- Are we using our limited resources in the optimum way to mitigate cyber risk?
- Is our cyber insurance coverage sufficient?
- What is the return on our cyber investment?

CRQ is revolutionising the cyber risk management function as organisations have started assessing risks quantitatively rather than qualitatively. Rather than just conducting a maturity assessment, quantifying cyber risks gives greater clarity with respect to hidden costs.

CRQ at work

Several methods are used for CRQ. Two of the most popular ones are Factor Analysis of Information Risk (FAIR) and the Monte Carlo simulations that calculate Value-at-Risk (Var).

The FAIR method breaks risk data into two quantifiable values: loss event frequency and loss event magnitude. Various forms of loss that the FAIR model considers include productivity, response, replacement, fines, competitive advantage, and reputation. The loss event frequency can be further divided into threat event frequency and vulnerability. Moreover, loss magnitude calculation has two parts − primary loss (loss within your organisation) and secondary loss (loss outside your organisation)

The Monte Carlo simulations use the probability distribution method to arrive at a quantified risk value. Most CRQ models work on the following equation:

Annual Loss Expectancy (ALO) = Annual Rate of Occurrence (ARO)*Single loss expectancy

A combination of loss event history, current and past risk assessment results, mathematical modeling, and business logic is used to calculate the exposure value in CRQ.

The method used to quantify cyber risk will depend on its purpose or use cases. The FAIR method is often used when extensive data is available in terms of industry, threats, etc. However, the Monte Carlo simulations are used when reliable data such as attack frequencies or losses, is unavailable.

The first step to implementing a CRQ solution in an organisation is by conducting a current state assessment and identifying a possible use case to test the waters. This will help choose the appropriate model for quantification.

Considering the complexity of risks and the system landscape of the organisation, organisations should have a technology platform. A few factors to be considered while selecting a platform is scalability, reliability, ease of use, integration capabilities, and cost.

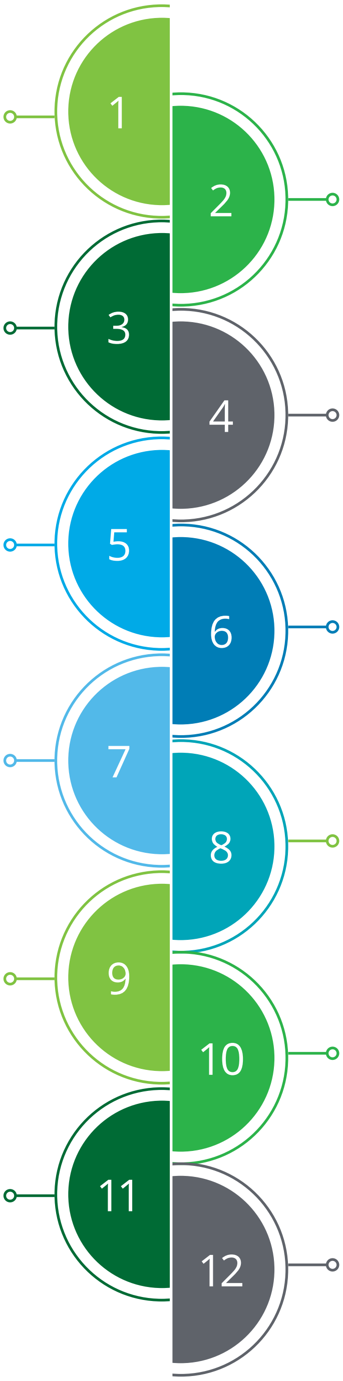
Some leading CRQ solutions enable various teams to simulate and see the impact of planned or current organisational controls on the total risk value. CRQ models help the operational team, including CROs and CISOs, and enable independent directors to make strategic decisions in terms of investments. The current trend shows a shift from maturity scoring models to more quantified risk models to assess cyber risk.

Different data sources considered for CRQ include SIEM, logs, SOC, root cause analysis, control effectiveness details and other GRC inputs, cyber threat intelligence data points, applicable regulations, and cyber audit findings.

Use cases for CRQ

Some challenges organisations face in implementing CRQ solutions include availability of quality data, changing threat landscape, regulatory requirements, and lack of understanding on which model to use.

However, CRQ can be deployed in organisations to solve key issues plaguing various functions. Some of these are mentioned below.



1. Ensure investment decisions on cybersecurity are risk-informed and have business value in terms of ROI (or measure effectiveness of cyber investments).
2. Cater to cybersecurity disclosure regulatory requirements from regulatory bodies, such as the SEC. The recent rule from the SEC requires the registrant to disclose the process to identify, assess, and manage cybersecurity threats. It also mandates disclosures on how the management reports cybersecurity risks to its board of directors/other committees.
3. Increase organisational resilience to understand the financial impact of an incident, thereby better preparing and responding to it.
4. Understand the impact of third-party risk on an organisation and curate effective measures to curb it.
5. Comply with various regulatory requirements by understanding the financial impact of cyber risk and taking steps to manage it efficiently and effectively and protect the organisation from penalties or regulatory scrutiny.
6. Present cyber risk to C-suite executives and the board of directors to enable them to have a risk-intelligent response to organisational risks.
7. Plan optimal resources internally to mitigate or manage risks.
8. Opt for the appropriate risk transfer option in terms of cyber insurance and look at the adequacy of cyber insurance coverage.
9. Understand the valuation for Mergers and Acquisitions (M&A) or Initial Public Offering (IPO) in terms of cyber due diligence.
10. Support business leaders with key decision-making for events such as new product launches and digital transformation projects.
11. Conduct scenario planning to identify efficient and effective risk treatment plans.
12. Perform risk assessments in more objective ways based on the quantified risk value.

Best practices to implement CRQ in an organisation

The following things should be kept in mind while implementing CRQ in organisations:

- Ensure that the CRQ model is always outcome-based. Start by quantifying the organisation’s top risks rather than looking to solve all problems in one go. Start small with a simple tangible use case solving some specific issues, such as budget allocation, cyber insurance coverage, or an investment decision, to ensure greater success.
- Create an asset inventory and map the threats and associated loss frequency and magnitude. Bring in inputs such as control effectiveness, industry benchmark data, incident logs, and regulatory requirements. This might help in quantifying risk.
- Identify the right partner who can help with technology and offer risk consulting services, as both are critical in the success of any CRQ project.
- Feed data such as internal and external threat landscape, control effectiveness, cyber risk appetite, business impact assessment reports, asset inventory with criticality rating, threat scenarios, and incident data into the CRQ model.
- Ensure that results or gaps of traditional maturity-based assessments are taken as an input to the CRQ models. The models can then look at scenario-based risks and try to quantify risk based on the information fed in, such as historical loss in environment, benchmarking information for the industry, other publicly available data.
- Build a persona-based intuitive reporting/communication layer to consume the quantified value of risks.

Conclusion

The beauty of CRQ is that it will not replace other risk assessment models but will co-exist with other qualitative models. This will help business leaders acknowledge cyber as a key business risk. They will support organisations' risk functions to move from reducing risk to optimising it and adding business value.

Although the adoption at present is at a nascent stage, this is where the future lies for CRQ. Organisations are currently taking the proof-of-concept route to see which model works best for them and what will get a buy-in from business leaders.

In the next 5-10 years, adoption of CRQ will increase and we will see collaboration amongst organisations, insurance companies, and regulators to assess and identify some insights that would help organisations effectively use CRQ models.

Connect with us

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Deepa Seshadri
Partner, Risk Advisory,
Deloitte India
deseshadri@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Joyce Rodriguez
Partner, Risk Advisory,
Deloitte India
joycerodriguez@deloitte.com

Tarun Kaura
Leader – Cyber Advisory,
Risk Advisory,
Deloitte India
tkaura@deloitte.com

Contributor

David George

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.