



# Guide to Cyber Risk Quantification

Learn How to Achieve Modern Cyber  
Risk Management

# Introduction

Organizations have been dealing with cyber risks since IT systems were being connected together in the 1970's, and [self-replicating malware \(e.g., worms\)](#)<sup>4</sup> were being unleashed. Decades ago, cyber attacks and “hacks” were isolated and esoteric. These days, they are endemic and affect core business operations for virtually every organization connected to the Internet.

However, even with this pervasive risk to an organization, cyber risk management is still an evolving space with several approaches and methodologies guiding professionals as cyber risks are assessed, communicated, and mitigated. Many organizations managing cyber risk rely on qualitative assessment approaches, often resulting in outputs that describe cyber risks in ordinal ways such as high, medium, and low, or numeric scores based on quasi-quantitative approaches. For instance, risk is often calculated by multiplying qualitative scores for the impact and likelihood of a cyber attack, like 1 to 5, which leads to a risk score. For example, if the impact score is 3 and the likelihood score is 5, the risk score would be 15. This approach is limited both by its subjective inputs and by its loose connection to business and financial metrics.

## Why Cyber Risk Management is Important

It is well known that as enterprises, government agencies, and other organizations embrace digital transformations and evolve their digital business strategies, their attack surface grows, creating new exposures used by threat actors for more successful attacks. For example:

- ♦ Ransomware payouts increased to over \$1.1 billion in 2023<sup>1</sup>
- ♦ According to IBM the average cost of a data breach in 2023 was \$4.45 million<sup>2</sup>
- ♦ Sophos' The State of Ransomware 2023 report indicated 61% of organizations had experienced a ransomware attack, with an average ransom cost of \$1.54 million.<sup>3</sup>

This leads to more attacks causing a variety of direct impacts to an organization, whether that's data confidentiality and privacy, availability of business-critical assets, or affecting human safety, and a disconnect between what the business does and how cyber attacks are managed, measured, reported on, and mitigated.

<sup>1</sup> [chainalysis.com/blog/ransomware-2024/](https://chainalysis.com/blog/ransomware-2024/)

<sup>2</sup> [ibm.com/reports/data-breach](https://ibm.com/reports/data-breach)

<sup>3</sup> [assets.sophos.com/X24WTUEQ/at/h48bjq7fqnp3n5thwxtg4q/sophos-the-state-ransomware-2023-infographic-1200-1200px\\_2x.png](https://assets.sophos.com/X24WTUEQ/at/h48bjq7fqnp3n5thwxtg4q/sophos-the-state-ransomware-2023-infographic-1200-1200px_2x.png)

<sup>4</sup> [fbi.gov/history/famous-cases/morris-worm](https://fbi.gov/history/famous-cases/morris-worm)

These factors challenge CISOs and cyber risk leaders to:

- ◆ Properly communicate cyber risks with leaders, executives, and boards of directors
- ◆ Determine risk mitigation strategies in the context of the organization's risk tolerances
- ◆ Adequately apply their budget and resources to mitigating the most critical risks
- ◆ Defend their risk mitigation decisions and investments to internal and external parties (e.g., auditors, regulators, partners)

The answer to these challenges is moving cyber risk activities and programs from qualitative, to quantitative. But first, let's explicitly define what cyber risk management is, and isn't, before diving into how to solve these challenges.

# What is Risk, Cyber Risk, and Cyber Risk Management?

## Let's start at the beginning, what is "risk"?

- ◆ A leading expert in risk management defines it as something that "... threaten things we value."<sup>5</sup> And what someone does about risks depends on the available options, valued outcomes, and belief about what might happen from each outcome (i.e., uncertainties).<sup>6</sup>
- ◆ NIST defines it in the context of manufacturing systems, but putting that aside, it's consistent with the various definitions across the industry.

"Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system."<sup>7</sup>

- ◆ The Institute of Risk Management adds the impact to an organization's reputation in their definition:

"'Cyber risk' means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems."<sup>8</sup>

It must be noted that a risk is not a threat. A threat is an event that leads to a risk being realized, e.g., a threat actor abusing a weakness in a system that leads to a data breach, system disruption, or damage, and ultimately has a financial impact on the organization.

<sup>5</sup> Fischhoff, Baruch, and John Kadvany, 'Defining risk', Risk: A Very Short Introduction, Very Short Introductions (Oxford, 2011).

<sup>6</sup> ibid.

<sup>7</sup> [csrc.nist.gov/glossary/term/cyber\\_risk](https://csrc.nist.gov/glossary/term/cyber_risk)

<sup>8</sup> [theirm.org/what-we-say/thought-leadership/cyber-risk/](https://theirm.org/what-we-say/thought-leadership/cyber-risk/)

Cyber risk management is the activities required to identify, assess, prioritize and manage the cyber risks to an organization.

Most organizations do some type of cyber risk management even if they don't have a formal cyber risk management program. It can be ad-hoc in reaction to an event, e.g., an attack against their digital assets, like a ransomware attack, or in response to an audit finding, like internal assurance audits or demonstrating compliance with an industry-standard like System and Organization Controls (SOC). It can be proactive as part of a one-off project to improve an

organization's resilience to cyber attacks or having a process to prioritize vulnerabilities to remediate.

Formal cyber risk management programs do all the above items as well, just in an organized approach where there is leadership support, a defined organization of cyber risk professionals, a dedicated budget for staff and required tools and defined procedures. However, the "how" cyber risk management is done is still a work in progress for many organizations. Its challenges primarily stem from the qualitative outputs, which is a legacy approach, yet the norm.

Cyber risk management is increasingly being formalized by organizations, but qualitative outputs create a number of challenges diluting its utility and value

## Common Challenges with Cyber Risk Management



### Spreadsheets

- ◆ What are my risks and how do I reduce their impact?
- ◆ What risks should I prioritize?
- ◆ How do I know if I'm spending money effectively?



### Effort

- ◆ It takes too long to assess cyber risks.
- ◆ There are not enough resources to assess all the risks.



### Data and Analysis

- ◆ Where should I start my analysis?
- ◆ Do I have the necessary data?
- ◆ Where do I even get the data?
- ◆ How do I know if my analyses are defensible?

# Quantification is the Key to Robust Cyber Risk Management

Cyber risk quantification (CRQ) can be defined simply as the means of defining cyber risks in financial terms. Sounds straightforward, but the field of CRQ, while being mentioned as far back as the 1990's, is still evolving, for example:

- ◆ In his 2007 book "Security Metrics," Andrew Jaquith places the context of his book about security metrics against risk management, saying "...risk means quantification and valuation."<sup>9</sup>
- ◆ In 2014, Jack Jones and Jack Freund released "Measuring and Managing Information Risk: A FAIR Approach," which documented the application of the FAIR approach to cyber risk.
- ◆ "How to Measure Anything in Cybersecurity Risk" was released in 2016 by Douglas W. Hubbard and Richard Seiersen<sup>10</sup>

While progress has been made in quantitatively measuring cyber risk, we're still in the early stages of making CRQ the de facto approach to doing cyber risk management.

Putting CRQ into practice has involved many approaches to "doing" risk quantification, for example - Do-it-yourself, FAIR, semi-quantitative, and more recently via AI and machine learning.

## Do-It-Yourself

This method for measuring risk is the concept of measuring risk by a proprietary method that is usually developed within an organization. In general, this is used after qualitative measurement methods are perceived as not being able to show value. A lot of the time this involves creating an excel spreadsheet or similar to help make risk actionable.

## FAIR

Factor Analysis of Information Risk, or FAIR,<sup>11</sup> was where the concept of measuring risk in business terms (dollars and cents) originated. This was the main crux that led to the creation of the OpenFAIR standard, which is an open standard from the Open Group. FAIR breaks risk down into probable frequency and probable magnitude to help determine future loss. This concept for measuring cyber risk paved the way for risk management teams to provide value for their organizations.

<sup>9</sup> Jaquith, A. (2007) Security Metrics. Pearson Education, p.3.

<sup>10</sup> How To Measure Anything In CyberSecurity Risk

<sup>11</sup> For more on FAIR visit the FAIR Institute ([www.fairinstitute.org](http://www.fairinstitute.org))

## Semi-Quantitative Measurement

Semi-quantitative measurement is a way of trying to add rigor to qualitative measurement methods. Usually, this is accomplished by establishing a risk score, for example; Impact score of 4 (high) and a Likelihood score of 3 (medium) = a risk score of 12. Generally, additional definitions are added to help determine what the “number” means.

## AI and Data-Powered

This is the newest way of assessing and measuring cyber risks. This generally is delivered as a commercial SaaS app used to perform the complex calculations needed to determine the risk and the amount of exposure faced by those risks, and how best to remediate risks to an acceptable level. This is usually accomplished by leveraging the MITRE ATT&CK framework to aid in this process. This is one of, if not the most efficient approach to performing cyber risk quantification.

# Common Use Cases for CRQ

Putting cyber risk quantification into practice is vital to ensure the investments in a cyber risk practice are realized. CRQ can support a range of use cases relevant to various teams and functions across an organization. Let's look at some of the popular CRQ use cases.

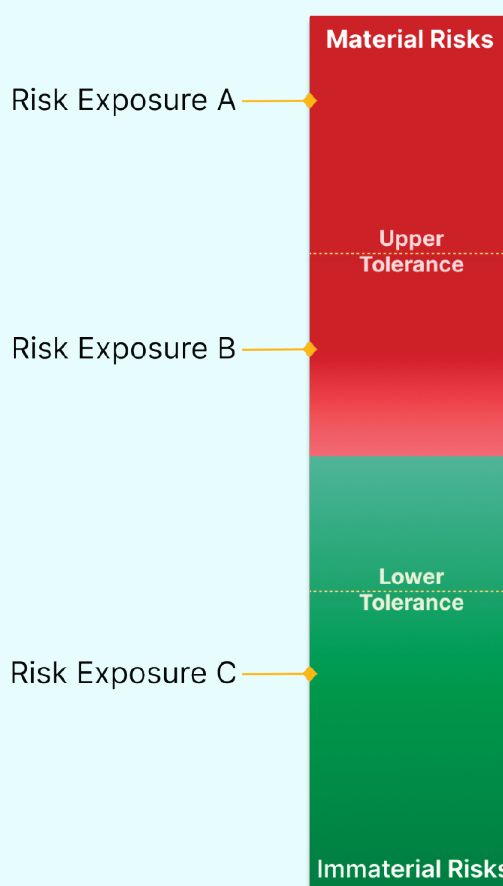
## Risk and Control Mitigation Prioritization

A top use case for CRQ is prioritizing controls investments to drive risk mitigation. Without quantifying risks, it's much more art than science when deciding which security controls will deliver the greatest risk reductions against your budget (monetary and people). Using CRQ allows cyber risk professionals and leaders to evaluate investments like their counterparts in the business, e.g., asking the question “If I have one dollar to spend, which investment is going to give me the greatest return in value?” When risks are quantified, it allows you to directly compare investments between competing opportunities, like do I upgrade my endpoint security or my network security tools?

## Defining SEC Materiality / Risk Appetite

Determining the risk appetite of an organization and what is a material risk is becoming an increasingly important question to be able to answer. For example, the 2023 U.S. Securities and Exchange Commission (SEC) rules on cybersecurity require publicly traded companies to demonstrate how they are strategically managing their cyber risks, and provide timely information to investors when a breach occurs.

The ability to define the risk appetite of an organization is vitally important when developing a cybersecurity and cyber risk management strategy, regardless of whether the SEC rules are applicable to your business. In the event of a breach, publicly traded companies need to know when an event is material to their business, which given the four business day notification window, is not something that an organization wants to be doing while responding to a breach. Defining materiality ahead of time is now a crucial part of breach and incident preparedness.



"Risk appetite is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision."<sup>12</sup>

## Improving Cyber Risk Communication

For many CISOs, communicating cyber risk to business leaders, executives, and directors is a constant challenge. Many leaders are not versed in cybersecurity and many CISOs tend towards communicating cyber risks in technical terms, not business terms. This has created significant friction between parties hindering effective communication, and the ability to properly discuss, agree, and manage cyber risks for an organization.<sup>13</sup>

<sup>12</sup> NIST SP 800-221 Enterprise Impact of Information and Communications Technology Risk, [nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-221.pdf](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-221.pdf)

<sup>13</sup> [hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity](https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity)

CRQ helps to break down the barriers between the parties by enabling the CISO to have risk conversations in the language business-leaders understand - money. It arms the CISO to be able to answer explicitly, and defensibly, how much a risk can impact the business in financial terms, and how much it will cost in monetary terms to reduce that risk. This dramatically changes the relationship between the CISO, and executives and directors, and removes the communication barrier enabling effective decision-making.

## Vulnerability Prioritization

Prioritizing which vulnerabilities to remediate is a proverbial issue for many organizations for a variety of reasons. Vulnerabilities are numerous, and their numbers are growing.<sup>14</sup> This creates significant friction within the cybersecurity team as well as other stakeholders, like IT and business application owners.

The challenge the vulnerability management team and cyber risk managers face is again an economic one: which investment in resources is going to give me the greatest return? Said another way, if I can only invest in remediating five vulnerabilities this month, which ones are going to reduce the greatest amount of risk?

The issue is that current approaches to prioritizing vulnerabilities are generally qualitative, with some evolution towards semi-qualitative occurring. Many vulnerability management analysts rely on scoring systems from their vendors, which provide qualitative measures, even if they appear to be quantitative-like. For example, there are proprietary scoring systems as well as industry-driven ones like the Common Vulnerability Scoring System (CVSS)<sup>15</sup> and the Exploit Prediction Scoring System (EPSS).<sup>16</sup> The issue is that while these scoring systems are improvements on purely qualitative approaches, like using high, medium, or low, they still lack the business context like the criticality of the asset or the asset impact on a business process. It also leads to scenarios where current scoring systems create conflicts, like what happens if there is organizational capacity to remediate 10 vulnerabilities this month, but there are 20 vulnerabilities that scored a 10 out of 10?

- ◆ How do you decide which ones to remediate?
- ◆ How do you explain to leadership your decision?
- ◆ How do you justify additional resources to remediate the additional 10 vulnerabilities?
- ◆ How do you demonstrate that you are even remediating the most critical vulnerabilities?

Even the best organization doing vulnerability management may face these questions. This is where CRQ makes a difference.

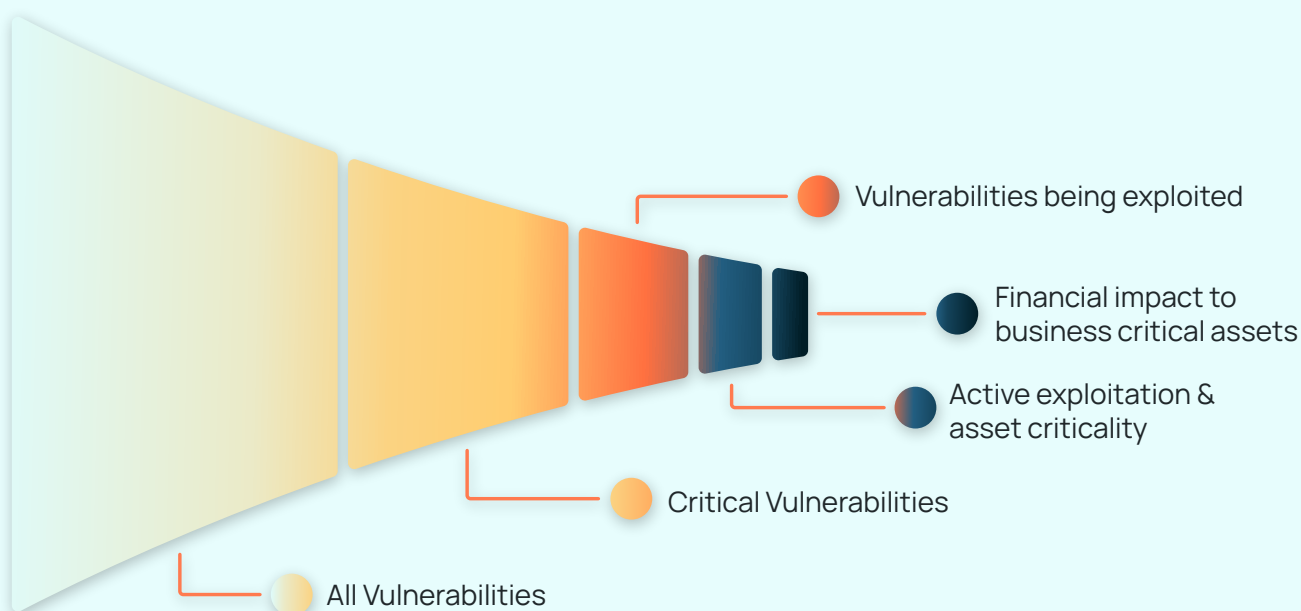
<sup>14</sup> [infosecurity-magazine.com/news/2023-26000-vulnerabilities-97/](https://www.infosecurity-magazine.com/news/2023-26000-vulnerabilities-97/)

<sup>15</sup> [first.org/cvss/v4-0/](https://first.org/cvss/v4-0/)

<sup>16</sup> [first.org/epss/](https://first.org/epss/)

CRQ provides the potential financial impact to business assets, allowing the vulnerability management team to know which assets are truly business-critical (i.e., they have the highest financial impact to the business). This allows them to invest in remediating vulnerabilities that will generate the greatest risk mitigation return on investment, and having discussions with leadership on allocating more resources based on their risk tolerance. Leveraging financial impact data removes the emotion from decision making between parties because the choice of assets to remediate is defensible – monetary impact to the business if that vulnerability was exploited and used to breach the organization.

## Vulnerability Assessment Funnel



## Third Party & Supply Chain Risks

To operate their companies, businesses are increasingly reliant on digital supply chains, traditional physical supply chains, and third party services providers. For example, the average organization uses 130 SaaS apps.<sup>17</sup> Managed services are crucial for many organizations across a variety of functions, especially in IT with the increased use and reliance on cloud services like AWS, Google, and Microsoft, but also for business processes like accounting, payroll, human resources, customer support, and more. Adversaries know this, and are taking advantage of this reliance on third parties. One of the most visible examples is the attack against Solarwinds<sup>18</sup> that led to the compromise of over 18,000 customers, enabling attackers to gain access to these customers' environments. This is surely not the last time we'll see an attack of this sophistication and magnitude.

<sup>17</sup> [bettercloud.com/monitor/the-2023-state-of-saasops-report/](https://bettercloud.com/monitor/the-2023-state-of-saasops-report/)

<sup>18</sup> [ciscuresearch.org/solarwinds](https://ciscuresearch.org/solarwinds)

The challenge, against this backdrop of high-impact attacks happening against the digital supply chain, is how to adequately manage supply chain and third party cyber risks. Many organizations lack the resources to perform this critical function, while organizations that have made the investment are still doing supplier risk management manually (e.g., with surveys and spreadsheets) and qualitatively (e.g., using ordinal scales and ranking). This leads to the usual challenges covered in other use cases:

- ◆ How do you prioritize the cyber risk impact of one supplier over another?
- ◆ Is the data you're collecting and using defensible?
- ◆ If two suppliers have the same level of cyber risk to the organization, which do you prioritize if you could only help mitigate one?

Cyber risk quantification can play an important role in supply chain cybersecurity, similar to the other use cases mentioned. CRQ:

- ◆ Enables risk managers to know which business assets (and processes) are most critical to the organization
- ◆ Provides organizations with a standardized approach to assess and compare the security posture of different suppliers
- ◆ Allows risk managers to effectively communicate with leaders and executives in business terms, improving collaboration and risk decision making

## Compliance with Regulations and Frameworks

The need to comply with regulations and frameworks is not abating any time soon. Regulations are increasing around the world, while customers and partners are requiring more transparency and evidence about an organization's cybersecurity program. In the U.S. the SEC cybersecurity rules were implemented to provide investors with more transparency about publicly traded companies' cybersecurity strategy and breach events. NIST's version 2 update to the Cybersecurity Framework adds Governance as one of the core pillars of the framework.<sup>19</sup> The updates to ISO 27002:2022 have refined the recommended information, cybersecurity, and privacy controls organizations should adopt in a more standalone framework.

Demonstrating how an organization complies with one or more of these regulations, and with various frameworks, can be a challenge. This is where CRQ plays a role. When the financial impact of attacks is understood, it makes allocating investments in security controls demonstrable and defensible, whether it's net new controls, updating controls, or removing redundant controls. It's easy to show how an organizations' cybersecurity strategy is aligned to security controls, and the coverage of those controls relative to frameworks.

<sup>19</sup> [nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf)

## How Do You Communicate That an End of Life (EOL) System Should Be Retired?

Many companies, large and small, have legacy systems that they are working to retire in favor of more modern, secure solutions. These legacy systems can be past their end of life (EOL), have vulnerabilities or technical risks that can't be patched, and aren't being maintained. Yet there is still a struggle to retire these systems as they have been, and continue to be, critical to certain customers, partners, and integrated systems.

Calculating the financial risk that an older system brings to the business is a key way to ensure its timely retirement. Many companies use CRQ to show that the financial risk of the older system is much larger than the newer system. CRQ helps to enable the business to make the decision to retire the system due to the financial burden, not technical risk metrics, that exist.

### Exception or Gap Management




Many companies have a process for making changes to their IT environment. These changes typically involve a set of decision makers across the business, IT and security discussing the benefits of the change and whether the requirements in the system meet the company's guidelines.

Often those guidelines, especially when it comes to security, aren't met and the team is left with a challenging decision - do they allow the change to be made, knowing that security isn't up to the guidelines - or do they stop it and impact the business? In many cases the business can show the financial impact of a delay and a waiver is granted.

But few companies know what the impact of those exceptions, or gaps in coverage, add up to. Companies using CRQ can calculate the financial risk of those exceptions before they are granted and allow security to say "yes, you can have the waiver if you accept this financial risk". Changing that conversation enables the business to understand the value of security and the risk of waivers, thus lowering the potential financial impact they face.

## Addressing the Challenges Implementing a CRQ Program

It's important to remember that whether you are looking to build a CRQ program, or operationalize and mature an existing one, it's a journey that takes time, effort, and investments. That journey starts with getting started, evolves into providing value, and finally achieves integration into business risk processes.

	 <b>Getting Started</b> 01	 <b>Providing Value</b> 02	 <b>Process Integration</b> 03
<b>Objective</b>	Establish a desire to have CRQ like Output	Provide value to decision making, working towards maturity by showing tangible value	Integrate into the businesses risk process and measure financial cyber risk continually across the business
<b>Getting Started</b>	Start small. Run a high level analysis of your company and 1 scenario that you know your company faces. Socialize the results.	Start using CRQ to make decisions. The next time a program wants to make a change to the IT baseline, analyze what the cyber risk would be, the mitigations, and the ROI. Present that at an approval meeting (Change Board or other type.)	Automate CRQ into your GRC or CMDB so that when the technical environment changes (or a risk assessment is complete) you can view the associated financial risk.
<b>Timeframe</b>	1-2 weeks	2 - 4 weeks	Continuous
<b>Use Cases</b>	Risk assessment in an ad-hoc manner.	Prioritize investments. Measure the financial impact of 3rd parties.	Continuously measure cyber risk for unexpected threshold exceedance.
<b>What Do I Do With The Data?</b>	Show it to the CISO. Then show it to the business owner (who owns the scenario you created.)	Incorporate it into the process of making changes to applications or for granting security waivers.	Make it part of every Board conversation and investment decision your company makes.
<b>What Questions Will They Ask Me?</b>	They'll ask things like "how did you get your numbers? How did you do this? Where did you get the data? What am I supposed to do with this?"	They'll ask things like "can I get a waiver if I'm not compliant or can't meet security?" And you get to say "Yes, if you accept this financial risk"	At scale you'll be asked things like "Are we optimizing investments across the business?", "Are we insured properly?", and "What else should we do to manage risk?"
<b>Outcome</b>	That last question - "what am I supposed to do with this" is the key question. The answer is: <ul style="list-style-type: none"> <li>Analyze your application in more detail (if you haven't already)</li> <li>If you have, run What-If scenarios to see what changes they can afford to invest in and ones they must invest in</li> </ul>	Tradeoffs are made using CRQ. When a decision comes whether to: <ul style="list-style-type: none"> <li>Invest in a new tech</li> <li>Upgrade a system</li> <li>Add a new feature</li> </ul> CRQ data is key to understanding how, where, and when cyber is applied	CRQ is now part of the up front decision making process for the organization vs. being done after the fact. You've matured to be the point of being integral to the financial parts of the business.
<b>Stakeholders</b>	<ul style="list-style-type: none"> <li>CISO</li> <li>Business Owner</li> </ul>	<ul style="list-style-type: none"> <li>CISO</li> <li>Business Owner</li> <li>Risk Team</li> </ul>	<ul style="list-style-type: none"> <li>C-Suite</li> <li>Risk Team (ERM or other)</li> </ul>
<b>How Do I Define Success?</b>	They ask you to keep going. Do more.	You begin to use CRQ to make actionable decisions. People ask for CRQ data as part of their decision processes.	Cyber risk quantification is baked into the fabric of your risk management process.

For organizations embarking on this journey, it's important to consider the following:

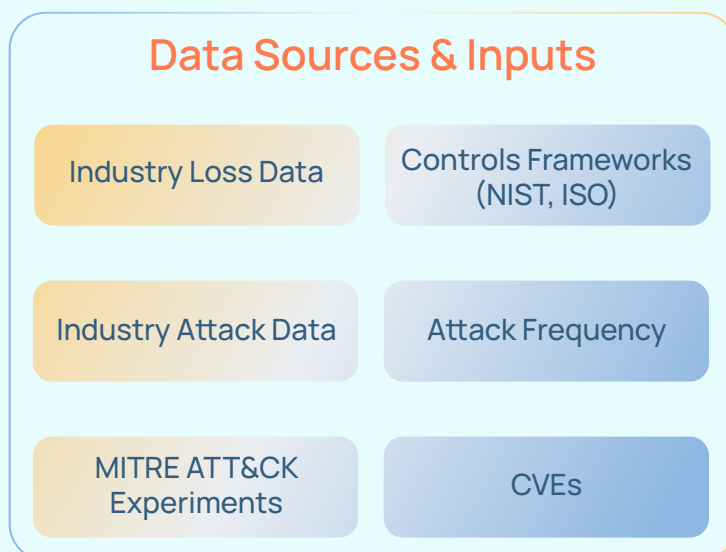
- ◆ Leadership/executive support is critical. If there is no top-level support for the program, the rest of the required components will be a struggle to address, and not just because there may be a lack of funds. It can make influencing internal resources harder to prioritize your needs.
- ◆ Organization dynamics need to be considered and addressed. It raises questions about:
  - ◆ Where will the cyber risk team report to in the organization?
  - ◆ Who will build and lead the function?
  - ◆ How will the function be staffed?
- ◆ You can't do CRQ without staff. People are a critical element of the program and a CRQ program will require professionals with specific skills and knowledge about cyber risk, threat modeling, etc. along with soft skills like communicating with both technical and business personas.

- ◆ Operating procedures and processes need to be defined, both within the CRQ team, and with stakeholders across the organization.

- ◆ Building and sustaining a CRQ program is dependent on having the right data. A CRQ program will require a variety of data types, such as historical loss and cyber attack data for your business' industries, knowledge of the frequency of cyber attacks, and vulnerability data (e.g., common vulnerabilities and exposures (CVEs)). There is also contextual information such as risk and security control frameworks like NIST 800-53, NIST Cybersecurity Framework, and ISO 27001/2, amongst others, and MITRE

ATT&CK for describing threat actor behaviors and doing threat modeling. As it's likely becoming obvious, the amount of data required is significant. It has to be collected to start a CRQ program. There also needs to be a process in place to continually capture new data and changes (like when control frameworks are updated), and make that data usable.

- ◆ Knowing which CRQ approach is "the best". There is no industry standard "best practice" for doing CRQ. The FAIR approach discussed earlier has been in use the longest in the field. Still, it has its challenges and limitations, primarily the overhead required to use it, the inability to scale, and its lack of defensibility. This has led to quasi approaches, like semi-quantitative or Semi-FAIR, and for some organizations to build their own approaches. Again, these models face the same challenges as FAIR. The more modern approach is an automated, data-driven analytics one that removes the deficiencies of the above approaches. However, deciding the right approach for your CRQ program must be identified at the beginning to determine the program needs and requirements across people, processes, and technology, and for organizing the CRQ function.



Finally, but no less importantly, having the right technical solution to bridge people and processes. A CRQ program needs a solution to drive it. The question is, what are the characteristics of that solution. The tools used to do risk quantification include:



### Spreadsheets

A very common option. Simple to implement, but expensive to maintain and they don't have the ability to scale along side a CRQ program.



### Custom-built, proprietary applications

Another popular option for organizations with large budgets and access to experts in threat modeling, risk quantification, data science, and AI engineering.



### Purpose-built, commercial solutions

This is the traditional route for many organizations once they graduate out of using spreadsheets. There are a variety of apps on the market, with most focused on enabling FAIR assessments, and modern apps that take a post-FAIR approach.

## Debunking CRQ Misconceptions

There are several common misconceptions about cyber risk quantification that have emerged over the last decade, and are important to address and debunk.

### 1. Quantifying Risk isn't Possible

Organizations have been trying to understand their cyber risks for many decades. The challenge they keep facing is that quantifying risk isn't possible so they tend to stick with qualitative scales: Red, Yellow, Green or High, Medium, Low. The problem is that these scales are not actionable, so the risk teams providing these ratings were perceived as not providing value. Since that perception was that Cyber Risk Quantification was not possible, that is where FAIR entered the scene. FAIR fundamentally debunked the skepticism that cyber risk quantification isn't possible.

## 2. Cyber Risk Quantification is Too Hard

The FAIR model is great, however one of the main challenges with it is that organizations feel it's just too hard or takes too long to perform an analysis. In short, it comes down to a people problem. Sometimes people are forced into a "risk" role without truly knowing what that actually requires. Not to mention expecting someone to perform a role that requires thinking outside the box. Since the advent of the FAIR model, organizations like the FAIR Institute have worked to make the risk analysis process easier, through offering training and services, for example.

## 3. FAIR is the Only Option to do Cyber Risk Quantification

In cyber risk quantification people tend to think FAIR is the only way to do quantitative analysis. While this had been true for a few years, that is not the case anymore. Now CRQ vendors can leverage machine learning/AI to help perform cyber risk quantification. This not only makes it easier but faster and more defensible.

## 4. Cyber Risk Management Ends with Quantifying Your Risks

Some organizations tend to think that once you quantify your risks you are done, however that is simply not the case. The lifecycle of a risk goes far beyond just quantification. The risk management process goes from identification through to monitoring.



This means in order to have a successful cyber risk quantification program (or risk quantification program in general) an organization needs to develop an end-to-end process that will ultimately lead to risk decisioning. In other words, ensuring that the risk (cyber) program is providing continual value to your organization by making effective risk management decisions.

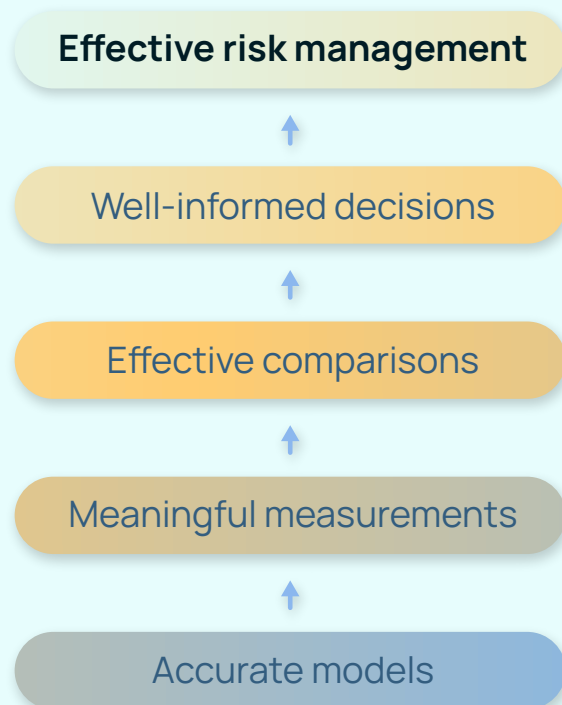
<sup>20</sup> [fairinstitute.org/blog/4-small-steps-to-get-started-with-risk-quantification](https://fairinstitute.org/blog/4-small-steps-to-get-started-with-risk-quantification)

## 5. My Organization is Not Mature Enough to do Risk Quantification

This is a very common misconception. Organizations feel they either don't have enough or need better data. While there is some validity to this, it is also not completely true either. Generally, this myth is rooted in the fact that they are trying to quantify everything they have. They hear the word CMDB and think "Ours is not good enough, so therefore we can't do cyber risk quantification". In reality, just like any risk analysis it can be seen as an iterative process. Risk analyses are completed at a specific point in time. It is important to remember that one small step forward (towards quantification) is one step further than you were. Your data can evolve over time. Start with what you have or what you know. Accuracy over precision when you are starting out. Making risk-informed decisions is the goal. No one has a crystal ball so there is always going to be a little room for improvement, but it also allows you to determine when enough is enough. JUST START.

## 6. Quantifying Cyber Risk is Too Time Consuming and Inefficient

Performing a CRQ analysis faster and more efficiently has been the goal of CRQ since people have figured out that measuring cyber risk is possible. Organizations want data, and not just any data, data that can be leveraged in an automated fashion to make it functional and easy to use. This is where the convergence of data science and industry data comes into play. Taking known events to help determine what would be a statistically reasonable forecast for how often and how much an event would cost the organization. This is only part of the equation. The other part is determining the frequency and loss against an asset. This is where machine learning and AI can really help. Someone once said there is nothing new under the sun, this goes the same for cyber criminals. The data shows them using similar techniques to get the end goal of a data breach, ransomware or DDoS attack. They sometimes even use multiple techniques to achieve their goal. Determining what the most effective attack path based upon an organization's controls is where AI and machine learning is needed. This allows a much more efficient approach to determining the loss exposure for an organization because it takes the guesswork out of it using data.



# Putting CRQ into Practice

Like any program or function, a combination of people, processes, and technologies are required to support a variety of use cases.

When putting cyber risk quantification into practice, all three – people, processes, and tools – are vitally important to address. Choosing the right technology to use will have an impact on the effectiveness of the people and processes involved in the program, and success of meeting the goals of the use cases and achieving the desired outcomes.

## ThreatConnect Risk Quantifier (RQ): The Market-Leading Solution to Help You Operationalize CRQ

### ThreatConnect RQ solves the challenges with CRQ.

- ◆ Removes the need for collecting, processing, and maintaining the data required to produce robust cyber risk analysis outputs. RQ does all the data collection and management heavy lifting so you don't have to worry about it.
- ◆ Provides fit-for-purpose AI and ML-powered analytics that have been tested and vetted to make cyber risk analysis faster and easier, without needing to be a deep subject matter expert in data analytics and cyber risk.
- ◆ Extensible to your preferred approach to quantifying cyber risk, whether that using FAIR, Semi-FAIR, our proprietary models, or custom models, allowing you to evolve your current CRQ approaches over time.
- ◆ Leverages industry standards and frameworks, such as ISO27002, MITRE ATT&CK, and others as part of the security controls analysis, and automating recommendations on coverage and configurations to generate the highest return on risk mitigation investments.
- ◆ Provides defensible financial impact outputs, enabling you to have effective cyber risk conversations with application and business owners, executives, and directors, leading to improved decision making on risk management and mitigation.
- ◆ Enables easier compliance with industry frameworks and regulatory requirements, such as knowing what constitutes a material impact for the SEC cybersecurity rules in the U.S., and to always be audit-ready when addressing internal, external, and third-party audits.

# Learn How to Start or Evolve Your CRQ Journey

Thanks for taking the time to learn about how to put cyber risk quantification to work in your organization. If you'd like to learn more about cyber risk quantification or ThreatConnect's RQ solution, please visit [threatconnect.com/RQ](https://threatconnect.com/RQ) or reach out to us at [threatconnect.com/request-a-demo](https://threatconnect.com/request-a-demo).



ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets. Learn more at [www.threatconnect.com](https://www.threatconnect.com).

ThreatConnect.com  
3865 Wilson Blvd.,  
Suite 550  
Arlington, VA 22203  
[sales@threatconnect.com](mailto:sales@threatconnect.com)  
1.800.965.2708