ThreatConnect.

Whitepaper

Operationalizing Cyber Risk Quantification

The Value of Understanding the Financial Impact of Cyber Risk

Foreward

New Gartner research shows that 88% of board of directors regard cybersecurity as a business risk.[1] This is excellent progress for security teams that were once siloed, as it catapults their importance and the impact they can have in securing the future of the business. As businesses become more dependent on technology to provide their goods and services, new risks will continue to emerge, presenting a myriad of significant challenges for security and risk professionals.

Being able to discuss cyber risk through the lens of financial impact and the monetary value is incredibly powerful, yet it is a skill that very few security professionals have mastered. The ability to understand the results of a successful attack or unpatched vulnerability can create great opportunities for organizations, allowing them to be proactive, agile, and resilient. By quantifying cyber risks, CISOs can better address the biggest dilemmas they face today.

Let's look at some practical ways you can get started with cyber risk quantification (CRQ) to create meaningful and actionable outcomes.

Unsure of how to **translate business cyber risk into financial terms** that stakeholders understand? Here are some ways to operationalize cyber risk quantification.

- **Prioritize what matters most**
- **Invest in strategic relationships**
- **Don't be afraid to start with small steps**
- **Create a plan for cyber risk maturity**

Jerry Caponera

General Manager of Cyber
Risk Quantification Products
ThreatConnect

[1] Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk

01

Start With What Matters Most

Unless you already have strong business partnerships across your organization and an unlimited budget, it can be challenging to decide where to begin to quantify cyber risk, and getting cross-functional buy-in can be daunting. After all, there are many critical business tools you could profile, build business cases for, and create security scenarios around in financial terms. Just about every new product or service leverages technology that introduces cyber risks, and realistically it's often not possible to address them all. Keeping that perspective in mind can help simplify your approach to getting started so that you don't spend time trying to translate every single risk into a monetary figure. Instead, be selective about your battles. Pick the risk that matters most and start there.

In order to associate cyber risk with a monetary value that would resonate with your organization's business leaders, start by asking yourself:

- Which applications would have the highest impacts if they were no longer accessible?
- Which applications hold the most sensitive data or could cause damage if accessed by an unauthorized party?

Risks can impact businesses in various ways, so context should be a key consideration. For example, an online retailer could not afford to have their site offline, which would hinder revenue generation. A healthcare provider would not be able to have IT systems offline, as it would prevent them from accessing patient medical data. A manufacturer would not be able to produce goods at total capacity if production lines were tampered with.

One European study suggested that up to 80% of an organization's value comes from intangible assets (for example, human capital, intellectual property, and reputation).[2] On the flip side, you have digital initiatives that are subject to GDPR and similar legislation, where a qualifying breach could result in an organization being fined as much as 4% of its global income.[3] In order to find a balance between these equally important considerations to avoid operational disruption, data breaches, legal or reputational impacts, CISOs must build relationships with business leaders across the organization. Unfortunately, cybersecurity is often too much of an afterthought or not even considered at all. Often it comes with a tarnished reputation as an obstacle to projects moving forward, and overcoming this perception can be challenging.

One study found that **81% of organizations** had indicated that they sidestepped cyber processes and **did not consult cybersecurity teams at the planning stage** of new business initiatives.[4]

Because of this perception, security teams often have limited involvement and visibility into what gets deployed. Most cybersecurity professionals admit that organizational business units frequently launch applications, customer experiences, and digital services that they know nothing about. Against the backdrop of challenges like this and an ever-changing cyber threat landscape, let's look at the steps you can take to identify and quantify your cyber risks.

[2] The Role of Intangible Assets In The Modern Cyber Threat Landscape, The Hermeneut Project

[3] What are the GDPR Fines? - GDPR.eu

[4] EY Global Information Security Survey 2021

Invest in Strategic Relationships

Once you've recognized the opportunity to improve your security posture by quantifying cybersecurity risks proactively, you might be asking yourself how you can communicate and cement the importance of cybersecurity within the rest of the business. The best place to start building a risk awareness culture is to start at the top and focus on what's in it for everyone. You will most likely need to gain buy-in from business stakeholders who are responsible for overall profit and loss, new product innovations, and customer success.

In a recent EY survey, 59% of security professionals indicated the relationship between their organization's security teams and lines of business were at best neutral, mistrustful, or even non-existent.[4]

Of course, if you already have a good working relationship with your organization's business leaders, your job becomes easier. If not, look for opportunities across business units to work together and ask yourself, "What's in it for them?"

You'll need to understand and align with business leaders' multi-faceted goals and challenges. This provides an opportunity to tailor how you communicate the importance of cyber risk for their objectives and how actionable outputs from understanding these risks can help reduce it. In addition, this creates an opportunity to position yourself as an enabler and an ally, so they are more likely to accommodate cyber risk considerations into their business strategies and developments. Here are some examples:

- **Highlight the importance of digital infrastructure plans and demonstrate the cost associated with a loss of corporate communications or application downtime.** Show this by the minute/hour/day and how it will impact the company's revenue streams.
- **Help business leaders build the business case for moving away from antiquated 2-factor authentication and annoying CAPTCHA techniques and move towards more sophisticated forms of AI, behavioral, and identity verification techniques that increase customer engagement.** While these solutions can be 20x or more the cost of simple CAPTCHA solutions, they are much more effective in both customer engagement and risk reduction.
- **Demonstrate to sales and marketing teams the importance of data protection. Avoid technical jargon and use examples that resonate with them.** For example, what would happen if a sales rep left a confidential client email on a train - what types of issues could this cause? Try an educational approach, establishing that partnering to drive down cyber risks empowers teams and resonates in a way that a general directive wouldn't.

AND THEN IF THEY STILL WANT TO BUY FROM US, LET'S SEE HOW WELL THEY CAN IDENTIFY BRIDGES.
TOM FISHBURNE
© marketoonist.com

[4] EY Global Information Security Survey 2021

Fun Fact:

It generally takes a human 32 seconds to complete a CAPTCHA challenge. There are 4.6 billion global Internet users. A typical Internet user sees approximately one CAPTCHA every 10 days. This is somewhere around 500 human years wasted every single day — just for us to prove our humanity.[5]

By using this scientific approach, the goal is to forecast issues before they arise. This way, your organization is prepared and confident if things pop up - which they almost always do. In the long term, employing a risk-based approach helps you identify opportunities and stay ahead of the competition.

Let's look at a practical example of this. Imagine a team within the organization wants to justify new UX features to enhance customer engagement with new services. It's important to know upfront and plan for the risks this could introduce. By harnessing CRQ, you can help ensure new features are implemented safely. Planning ahead for cyber risk exposure is a crucial element of the customer experience that should not be underestimated. These are successful strategies that support business partnerships and translate recommendations into action.

Ultimately, CRQ provides transparency for the financial impact of risks and elevates the importance of applications and digital services to an organization's value. The result? More budget for innovation and risk reduction can be an advantageous perspective to communicate when working with different business units.

Remember to revolve conversations around how cybersecurity can help justify more sophisticated technologies and, at the same time, reduce risk. The objective is to avoid conversations filled with fear, uncertainty, and doubt. Instead, have strategic conversations, align team goals with company goals, and make better decisions about new investments' risks and rewards.

Quantifying cyber risks provides an incredible opportunity to teach organizations how to put security first because it is the best way to operate due to regulations forcing compliance. Despite a strategic approach, if you find that cross-functional cooperation isn't there, it may be necessary to remind business leaders about fiduciary duty and personal accountability in potential D&O lawsuits. While these reminders provide a startling way to educate business leaders, it's certainly not the conversation you want to start with. Use these discussion points as a last resort tactic to establish buy-in.6 A great reference to use is the 2018 SEC guidance that now expects organizations to understand and be able to report the material risks associated with cyber threats in advance, even if they aren't currently affected by a specific cyber attack.

[5] CAPTCHA Can Kill Your Conversion Rate – Articles – Baymard Institute

[6] Commission Statement and Guidance on Public Company Cybersecurity Disclosures

[10] The Number of Data Breaches in 2021 Has Already Surpassed Last Year's Total, Fortune

[11] How Much Does a Data Breach Cost?, IBM

The financial impact of attacks is growing uncontrollably, the frequency of attacks is increasing, and security is overwhelmed with the quantity and variety of events to deal with. **The number of data breaches in 2021 soared past 2020's total10 by October alone, costing companies an average of $4.24 million each[11] and impacting millions of customers worldwide.** Waiting to quantify cyber risk is not a viable long-term option, so let's look at implementing a plan.

Cost of 2021 Data Breaches

Average of

$4.24M

As you form or strengthen strategic relationships, you may realize some applications or tools aren't under your purview, and you know nothing about them.[7] Some of your counterparts may have gone outside the ideal process to set up applications, but don't panic. Instead, look for cross-functional engagement opportunities to discuss the need for innovation, reducing risk, and better communication throughout.

There may be some situations for security teams to overcome if they want to solidify their credibility, so it's important to be mindful when approaching their counterparts in other departments. There are often existing applications, processes, and dependencies that are fundamental to the day-to-day of different departments, and communication can easily break down if this perspective is overlooked or dismissed.

Unfortunately, most cybersecurity teams have little or no relationship with most business functions — especially those involved in innovation, product development, and customer-facing activities.

- Almost three-quarters of organizations (74%) in a recent survey said that the relationship between cybersecurity and marketing is no better than neutral — and in many cases is indicated as mistrustful or non-existent.[8]

81% of organizations sidestepped cyber processes and did not consult cybersecurity teams at the planning stage of new business initiatives.[9]

- With remote working conditions, the percentage is even higher as things continue to happen too fast for security and risk reduction even to be a part of the conversation.[10]

Shadow IT is no longer a secret, everyone knows about it. Point out tools and be open to discussing different solutions. Use risk reduction to help them justify new and better technologies. Coming to a mutual understanding helps both parties reduce risk, provides more visibility to you, and allows them to continue working towards their goals.

[7] The $29 Million Yahoo Derivative Data Breach Settlement: What Next?

[8] Businesses consider cybersecurity as an afterthought despite growth in attacks, EY survey finds

[9] Allianz Risk Barometer, Allianz Global Corporate & Specialty

[10] The Number of Data Breaches in 2021 Has Already Surpassed Last Year's Total, Fortune

02

What Does a Mature Cyber Risk Program Look Like

Let's begin with the future in mind. What's at the end? A fully operational and mature Cyber Risk Quantification in your organization.

Characteristsics of a **Mature CRQ** Program Include:

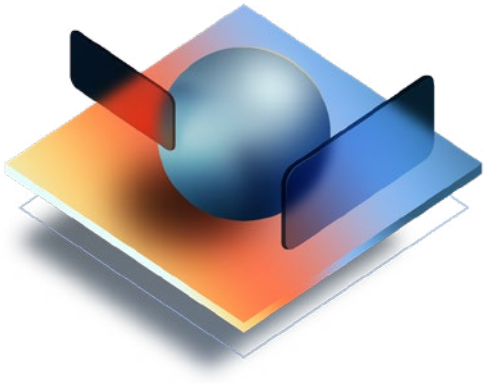
- Business owners, product line owners, legal and others discuss cyber risk in a common language
- Decisions are made around cyber risk mitigation and transfer with transparent financial implications (risk and ROI)
- Cyber risks seamlessly flow into the enterprise risk management process
- An exception process that can handle a newly defined cyber risk that exceeds the companies risk tolerance

That might seem like a daunting task, but by breaking down the characteristics of a mature CRQ program further, there are some fundamental building blocks needed to build a strong foundation.

Breaking it up into manageable pieces is a bit less intimidating to take on. The essential thing to realize is that you're not going to **convert the entire business to a well-oiled CRQ machine overnight.** But you can provide value today with CRQ, all while building towards a combined end goal of protecting your organization.

Key Elements You'll Need:

- Capturing cyber risk in financial terms
- Building a clear communication channel from security to business
- Company buy-in to having these conversations
- Measuring cyber risk regularly



03

Demonstrate the Financial Impact of Cyber Risks

Cyber risk assessments often start with long and detailed conversations with risk owners. Together, you must profile critical applications and tools used within the organization - How is it defended? What are the applications it is dependent on? Is sensitive data stored there - if so, how many records? That's where you start the third step of your organization's CRQ journey.

Imagine Being Able to Talk About the **Financial Impact of a Cyber Risk** in Terms a Business Leader Would Listen to:

$25M	**"A ransomware attack could cost us $25m in revenue."**
$1M	**"We could mitigate it with a $1m investment in Identify and Access Control that does away with our antiquated CAPTCHA techniques that have shown to lead to 33% user abandonment.[5]"**
250%	**"A ransomware attack could cost us $25m in revenue."**

CRQ isn't going to predict an increase in sales, but it can help business leaders justify better technology that reduces risk and improves customer engagement. If you are partnering with a business on their terms, find out what actionable results you can offer that align with their goals. If you still feel like you're not getting the support you need, here is an excellent question to keep the conversation going:

"If we don't make the $1M investment, who's willing to sign off on the $25M risk?"

This discussion style is paramount to influencing decisions about risk in the real world and what it means when it comes to actual financial impact. Because when all is said and done, it comes down to risk appetite and what they are willing to swallow.

[5] CAPTCHA Can Kill Your Conversion Rate – Articles – Baymard Institute

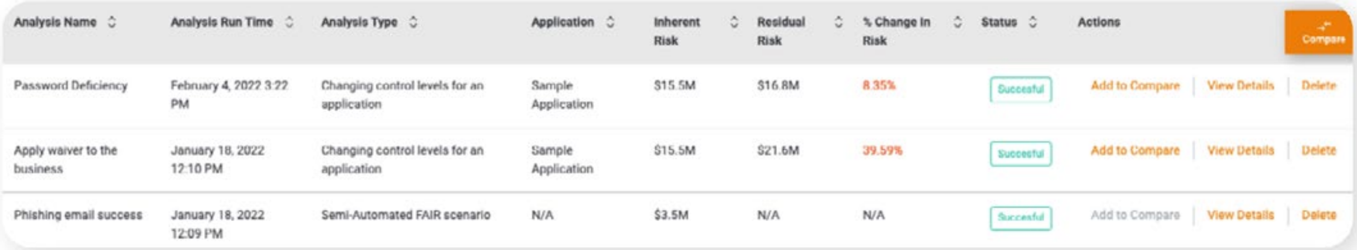
04

Integrate into the Business Risk Process

If we take a step back, most decisions are a choice between options. We can either go to the movies or the park. So, how would you influence decisions? If the decision was movies vs. the park, you could point out that there's a high chance of rain, so the park might not be a good idea. The question is, how do we do this for cyber decisions?

As a security and risk professional, you must explore multiple alternatives and determine the best one. The challenge with cyber is "what does best mean to the business"? This is where the financial calculations come into play. Say you're choosing between better endpoint detection or network detection. Which one should you choose? The endpoint team swears that they have the best tool since sliced bread. The network team believes they've found the holy grail that will help. How can you possibly get involved in that conversation?

Our suggestion is this: Don’t get involved in that conversation. Be the neutral advisor that uses data and finances to influence and make decisions. Show what can be done, but don’t dictate what must be done.



Analysis Name	Analysis Run Time	Analysis Type	Application	Inherent Risk	Residual Risk	% Change In Risk	Status	Actions
Password Deficiency	February 4, 2022 3:22 PM	Changing control levels for an application	Sample Application	$15.5M	$16.8M	8.35%	Successful	Add to Compare | View Details | Delete
Apply waiver to the business	January 18, 2022 12:10 PM	Changing control levels for an application	Sample Application	$15.5M	$21.6M	39.59%	Successful	Add to Compare | View Details | Delete
Phishing email success	January 18, 2022 12:09 PM	Semi-Automated FAIR scenario	N/A	$3.5M	N/A	N/A	Successful	Add to Compare | View Details | Delete

As shown above, option 2 provides better risk reduction. This doesn’t necessarily mean that option two is the best technology, however, it’s the best thing for the business. It’s time to start those conversations, provide factual financial data, and give your recommendations for their decision. It’s important to use data to tell the story that option 2 is the best solution, then let them decide. The easiest way for CRQ to get adopted is for its value to be cemented in the business. By being data-driven, you set yourself and the company up for success in the future.

05

What's Next?

Now that you've shown value to the business by helping them make decisions, you're ready to start moving your CRQ program to the next level. That means working across a larger portion of the business and delivering results to the entire organization.

Security is oftentimes an afterthought which leads to many security organizations operating on a fixed budget. Cyber risk is the fastest-growing risk faced by businesses globally. A wide range of statistics and sources make it clear that attackers have become even more proficient over recent years, using automation to exploit vulnerabilities at an accelerated pace and frequency. Threats are even more widespread and complex than before.

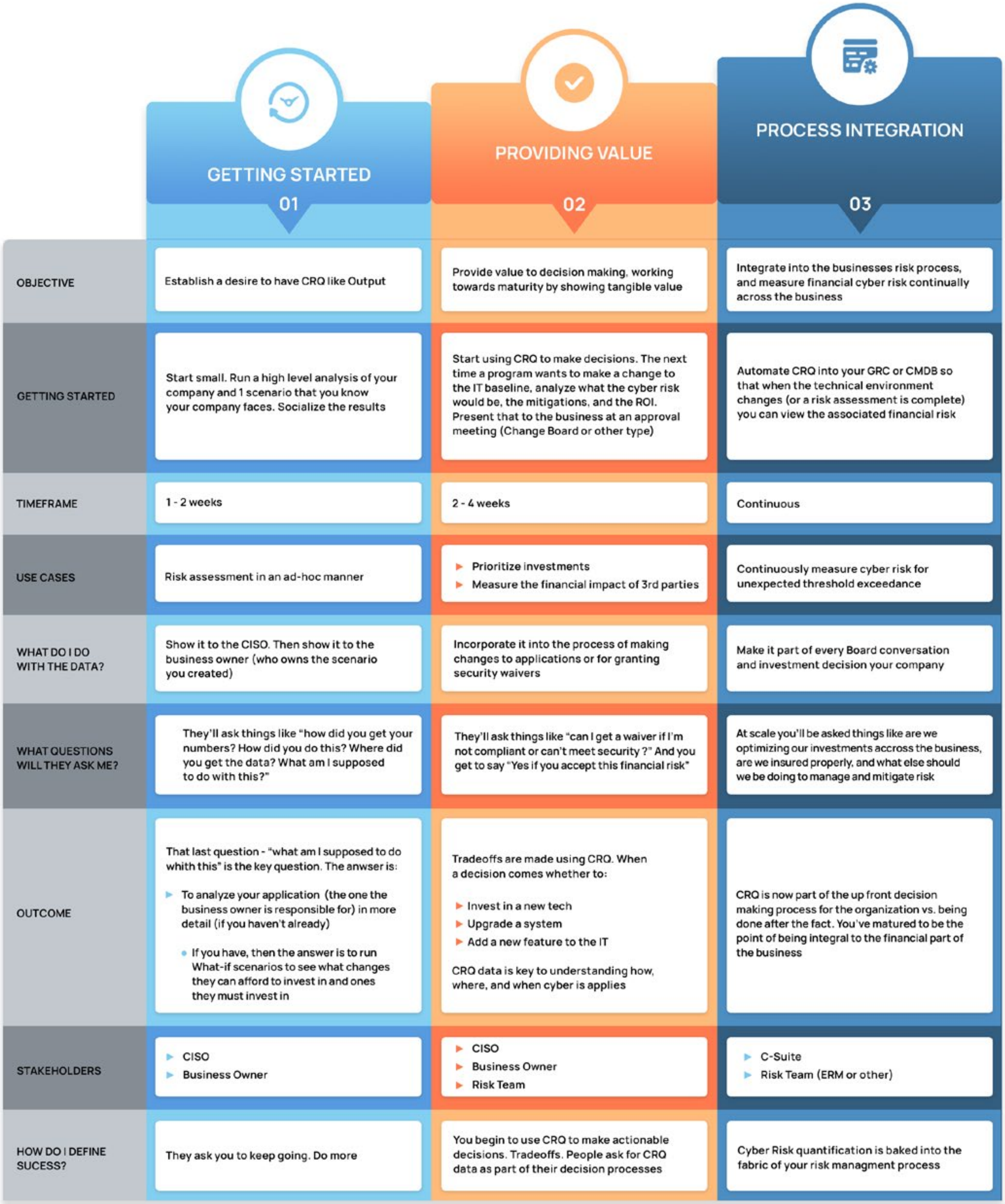
Consider This:

- 58% say their organization sometimes implements new technology with timescales that do not allow for suitable cybersecurity assessment or oversight.[9]
- Only 36% of organizations say cybersecurity is involved right from the planning stage of a new business initiative.
- 41% of security respondents describe their relationship with the marketing function as negative, up from 36% who said the same a year ago. At the same time, 28% say their relationship with business owners is poor, compared to 23% a year ago.[10]

A success plan defines the milestones, tasks, and guidelines needed for your CRQ effort to succeed. Quantifying cyber risk in financial terms will change how your business looks at security. Let the company mature your practice for you. After implementing a CRQ program, it'll be easy to see how it was the missing piece that bridged the gap between security and the organization. **By having security and business working from the same page, risk mitigation becomes the main priority – protecting the organization from harm.**

[9] Allianz Risk Barometer, Allianz Global Corporate & Specialty

[10] The Number of Data Breaches in 2021 Has Already Surpassed Last Year's Total, Fortune



	GETTING STARTED 01	PROVIDING VALUE 02	PROCESS INTEGRATION 03
OBJECTIVE	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
GETTING STARTED	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 to the business 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
TIMEFRAME	1 - 2 weeks	2 - 4 weeks	Continuous
USE CASES	Risk assessment in an ad-hoc manner	▶ Prioritize investments ▶ Measure the financial impact of 3rd parties	Continuously measure cyber risk for unexpected threshold exceedance
WHAT DO I DO WITH THE DATA?	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
WHAT QUESTIONS WILL THEY ASK ME?	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 our investments accross the business, are we insured properly, and what else should we be doing to manage and mitigate risk
OUTCOME	That last question - "what am I supposed to do whith this" is the key question. The anwser is: ▶ To analyze your application (the one the business owner is responsible for) in more detail (if you haven't already) • If you have, then the answer is to run What-if scenarios to see what changes they can afford to invest in and ones they must invest in	Tradeoffs are made using CRQ. When a decision comes whether to: ▶ Invest in a new tech ▶ Upgrade a system ▶ Add a new feature to the IT CRQ data is key to understanding how, where, and when cyber is applies	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 part of the business
STAKEHOLDERS	▶ CISO ▶ Business Owner	▶ CISO ▶ Business Owner ▶ Risk Team	▶ C-Suite ▶ Risk Team (ERM or other)
HOW DO I DEFINE SUCESS?	They ask you to keep going. Do more	You begin to use CRQ to make actionable decisions. Tradeoffs. People ask for CRQ data as part of their decision processes	Cyber Risk quantification is baked into the fabric of your risk managment process

About ThreatConnect

Changing the Way Security Works: Intelligence-Driven and Risk-Led

The ThreatConnect platform enables customers to drive operational and strategic decisions using risk quantification and threat intelligence. Risk Quantification (RQ) enables CISOs to lead the security function more defensibly and direct operational decision making with quantified risk in monetary terms; our integrated Threat Intelligence Platform (TIP) and Security Orchestration, Automation and Response Platform (SOAR) enable TI and SOC teams to make scaled, risk-aligned, and threat-informed decisions.

Reach out to learn how the ThreatConnect Platform can make you and your team more effective, decisive, and collaborative.

+1 (800) 965.2708 -or- **ThreatConnect.com/Request-a-Demo**

ThreatConnect.

ThreatConnect enables security operations and threat intelligence teams to work together for more efficient, effective, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse threat intelligence and cyber risk quantification into their work, allowing them to orchestrate and automate processes to respond faster and more confidently than ever before. Nearly 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their most critical systems.
Learn more at **www.threatconnect.com**.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203
sales@threatconnect.com
+1 (800) 965.2708