Definitive Guide™ to Cyber Risk Analytics

Measure Cyber Risks to Enable Your Business

Suzanne Porter-Kuchay
Jon Friedman

FOREWORD BY:
Landon Johnson

Compliments of:

NEHEMIAH SECURITY

About Nehemiah Security

Nehemiah Security works with enterprises around the world to elevate the security conversation and answer the question, “How does cyber risk impact my business?” Our mission is to deliver business-oriented intelligence on cyber risk so security leaders can integrate their operations into the suite of functions that corporations monitor and invest in every day. Visit nehemiahsecurity.com for more information.

Definitive Guide™
to
Cyber Risk Analytics

Suzanne Porter-Kuchay
Jon Friedman

Foreword by Landon Johnson

CYBEREDGE
GROUP

Definitive Guide™ to Cyber Risk Analytics

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at (800) 327-8711 or info@cyber-edge.com.

ISBN: 978-1-948939-04-1 (paperback)
ISBN: 978-1-948939-05-8 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco

Table of Contents

Foreword v

Introduction vii

Chapters at a Glance vii
Helpful Icons viii

Chapter 1: The Business Case for Cyber Risk Analytics 1

Cyber Risk Is a Business Problem 2
Boards are asking the hard questions 2
CISOs are struggling for answers 3
Why Cyber Risk Analytics? 4
Speaking in the business language 5

Chapter 2: The Power of Cyber Risk Analytics 7

What Is Cyber Risk? 7
Risk or threat? 7
Components of Cyber Risk 8
Three Approaches to Cyber Risk Analytics 9
Assessing risk with grades 10
Assessing risk at a technical level 10
Assessing risk with quantitative business metrics 10
More on defensibility 13

Chapter 3: Why You're Doing Cyber Risk Measurement Wrong 15

Current Methods Fall Short 16
Ordinal scales 16
Monte Carlo simulations 16
Four Common Mistakes in Measuring Cyber Risk 18
Thinking it cannot be done 18
Boiling the ocean with a match 19
Using unrelated data 19
Relying on stale data 20

Chapter 4: Cyber Risk: What to Measure, Where to Start 21

Let's Get Practical: Where Do You Start? 21
Find a champion 22
Focus on business priorities 22
Two Critical Metrics 23
Probability of loss 23
Computed loss 24
Three Sources of Data 25
Attackers 26
The IT environment 26
The business landscape 27

Overview of the Cyber Risk Quantification Process.......................................28
Modeling the business environment...28
Modeling the supporting IT environment.......................................28
Cyber risk quantification in four steps 29
The power of automation.. 30
Chapter 5: Making Decisions Using Cyber Risk Analytics...........................31
Adding Cyber Risk to the Risk Register 31
Communicating Cyber Risk...33
Now That We Have Your Attention: What Are the Options?..........................35
Risk response: what does risk appetite have to do with it? 35
Risk response strategies...35
Chapter 6: Mission: Possible 37
Become a Cyber Risk Champion...37
Set Yourself Up for Success...38
Automate with a cyber risk analytics tool 39
Your journey to cyber risk analytics leadership............................. 40
Mission Accomplished 40

Foreword

This Definitive Guide™ shares some of the best practices Nehemiah Security has developed while helping security and business leaders monitor and manage their cybersecurity risk. Cyber risk management is a critical topic that deserves far more attention than it has received to date, and we enjoy our role in leading the IT security community to a fuller understanding of the basic concepts and suggesting practical techniques.

As IT complexity continues to increase and attackers become more sophisticated and diverse, companies must make better-informed decisions about how to deploy their cybersecurity resources. If they merely react to headlines or the latest technology buzzwords, they could waste large portions of their security budgets and leave themselves open to data breaches and new types of attacks.

Most companies have existing processes for evaluating and comparing other forms of risk. Cyber organizations have yet to participate. That's because it has been (or at least seemed) too hard to translate technology-related risks into metrics that allow them to be calculated and ranked alongside other business issues.

Well, it's time for cybersecurity to join the party.

Industry thought leaders, including my colleagues at Nehemiah Security, have developed best practices for methodically assessing cyber risks in financial terms. These techniques enable organizations to practice risk-informed decision making and justify their decisions to CEOs, boards of directors, and business managers. In the end, they help to ensure that resources are optimally deployed to protect the company's most valuable assets.

This guide is for both security and business leaders.

Security leaders should dig into the details of how cyber risk can be calculated. This exercise will make it clear that evaluating cyber risk involves not only assessing technical challenges and the IT infrastructure, but also understanding attackers and the business environment.

Business leaders will learn why and how they should encourage their security teams to communicate in terms the business understands. This includes placing dollar signs on the potential impact to the organization, as well as on possible functional impacts (downtime, lost records) to the lines of business. Visibility into these potential impacts will help business leaders know where to spend their next round of cyber budget, and what they can expect from their investments.

We believe this Definitive Guide provides vital insights into the promise of cyber risk quantification. You will no longer be forced to accept red/yellow/green as a rating for your cyber posture. Instead, you will have a clear window into an entirely new and powerful world where security teams prioritize and communicate the value of cyber initiatives. Mastering cyber risk analytics takes some work, but cyber professionals who are dedicating their careers to protecting the highly valuable assets of their organizations will find the results to be well worth the effort!

Landon Johnson
Senior Vice President
Nehemiah Security

Introduction

Senior business leaders are asking themselves tough questions about cybersecurity, such as: “What are our top cyber risks?” and “Am I allocating my cybersecurity resources in the right areas?”

To answer such questions accurately you need a rigorous process to measure and analyze your cyber risk. As a security leader, you also have to communicate the results effectively to the business.

The majority of companies, however, measure cyber risk using simple risk measurement practices and generalized simulations. These speculative approaches make it difficult for security leaders to provide executives with the financially based metrics they need to make defensible decisions about how to deal with cyber risk.

This guide is intended to advance the conversation by providing practical advice on implementing financially driven cyber risk management. It will help you recognize the challenges associated with common risk measurement methods, as well as understand the power of cyber risk analytics and the value of adding cyber risks to the existing corporate risk register.

Even the most progressive companies are just starting their journey toward managing cyber risk effectively. This guide is designed to help you proceed down that path.

Chapters at a Glance

Chapter 1, “The Business Case for Cyber Risk Analytics,” discusses why cyber risk is a business problem and the challenges of communicating cyber risk.

Chapter 2, “The Power of Cyber Risk Analytics,” reviews the three components of cyber risk, approaches to cyber risk analytics, business benefits of cyber risk analytics, and the importance of defensibility.

Chapter 3, "Why You're Doing Cyber Risk Measurement Wrong," outlines why current cyber risk measurement methods fall short.

Chapter 4, "Cyber Risk: What to Measure, Where to Start," provides practical guidance on getting started and describes the risk quantification process, critical metrics, and the importance of automation.

Chapter 5, "Making Decisions Using Cyber Risk Analytics," explores the power of adding cyber risk to the risk register and how to frame cyber risk conversations.

Chapter 6, "Mission: Possible," examines how to set yourself up for success when delivering full transparency around cyber risk.

Helpful Icons

TIP

Tips provide practical advice that you can apply in your own organization.

DON'T FORGET

When you see this icon, take note as the related content contains key information that you won't want to forget.

TECH TALK

Content associated with this icon is more technical in nature and is intended for IT practitioners.

ON THE WEB

Want to learn more? Follow the corresponding URL to discover additional content available on the web.

Chapter 1

The Business Case for Cyber Risk Analytics

In this chapter

- Understand why cyber risk is a business problem
- Recognize the challenges of communicating cyber risk
- See why cyber risk analytics is a business imperative

"If no mistakes have you made, yet losing you are, a different game you should play."

— Yoda

It's a vicious cycle.

Hacker motivations have risen to new levels and now include espionage, disinformation, market manipulation, and infrastructure disruption. To achieve these aims, attackers have continuously upgraded their toolkits and techniques. In self-preservation, security leaders, once again, are asking for more funding.

Business leaders are left on the sidelines, wondering if this new round of cyber budget increases will protect their most valuable assets. But they have no real way of knowing.

Most organizations are operating blindly with respect to how much they are investing in cybersecurity versus the value they are receiving. As more—and increasingly serious—cyberattacks occur, corporate boards are beginning to doubt the effectiveness of current and proposed cybersecurity strategies.

Weary of ever-increasing security spend, business leaders are closely scrutinizing security budgets. Further, they are challenging the notion that cybersecurity remains solely an IT concern, rather than a function that must be fully embedded in the organization's risk management framework.

It's time to stop the vicious cycle of cyberattack → budget request → budget approval → repeat.

Cyber Risk Is a Business Problem

Cybersecurity teams have been forced to place a premium on action over strategy. Unrelenting attacks from unpredictable threat actors mix with gaps in the security team's understanding of the organization's business priorities to create this perfect storm of unaccounted-for cyber risk.

While security teams are fighting for survival of the organization, corporate leaders are making decisions at the highest level about where to expand, what offices to open, what partners to sign, and what systems to develop *without taking cyber into account*.

Boards are asking the hard questions

While no business leaders are saying "Do less to protect the organization," their attention has been drawn to the mounting cyber budget. Increased costs with unprovable ROI and marginal financial accountability have placed cybersecurity leaders in the hot seat for answers.

Unclear about the ROI and value of cyber spend to the organization, CEOs and board members are asking the same hard-hitting, intelligent questions they pose to every other leader in the organization. These are Business 101 questions, to be sure, and yet security leaders are poorly equipped to lead informed discussions with business leaders about managing cyber risk.

Critical Questions Boards Are Asking About Cyber Risk

- Why are we being asked for more money and resources?
- Are we cost-effectively and efficiently securing our critical business assets?
- Will our budget reduce our exposure to business loss to an acceptable level? What is an acceptable level?
- What is our current cyber risk to the business?
- Are we insured appropriately for the level of cyber risk we face?
- What strategic tradeoffs will we need to make to fund security initiatives?
- How should these tradeoffs be prioritized?
- Is this spend correctly prioritized in relation to all other business risk?

CISOs are struggling for answers

Security leaders continuously strive to help business leaders understand cyber risk. Cyberthreats and defense measures often dominate the conversation. These discussions can be reactive and, because of the level of technical language required, they can sound like Latin to the rest of the company. Business leaders are forced to translate these conversations into their own set of priorities, risks, and daily fires that they must manage. Frustrations grow as the language barrier and communication gap widens.

Boards speak the language of business and risk as opposed to cybersecurity and are holding security leaders accountable for doing the same. This is a struggle for most security leaders. It is not a lack of desire or capability that leads to this struggle; rather, it is the challenge inherent in translating technology-related risks into financially based metrics that can be ranked with all the other business issues.

An Example: Cyber Insurance

Organizations that are incapable of accurately calculating cyber risk are susceptible to making poor business decisions. One of the most immediate mistakes could be under- or over-investing in cyber insurance. This is a black box for most organizations. Spending too much obviously draws resources away from other needs. Spending too little can be catastrophic in the event of a cyber breach. Ensuring that insurance is aligned with cyber risk may not keep the company out of the headlines. However, it certainly could avoid an eight- or nine-digit price tag once the dust settles.

Why Cyber Risk Analytics?

To effectively manage their portfolio of risks, business leaders must understand how cyber risk impacts their organization.

Too often, however, cyber risk is measured using generalized simulations and Governance, Risk & Compliance (GRC) best practices or standards. This speculative approach weakens the credibility of a cyber risk story, and does not advance the cause for justifying budgetary needs for technology initiatives.

The time has come to measure, manage, and communicate cyber risk with verifiable intelligence and from the business perspective. Security professionals, however, aren't always comfortable talking about the business. The role of cybersecurity often focuses on technology-based needs. How many DDoS events were blocked? How many vulnerabilities do we need to patch today?

Security leaders need a way to communicate with business leaders—in very clear terms—the cyber risks of doing business.

The answer lies in cyber risk analytics. Cyber risk analytics provides a data-driven methodology to connect the dots between business applications, IT exposures, vulnerabilities in technical assets, and known-attacker scenarios to quantitatively measure security risk and potential losses in financial terms.

Speaking in the business language

Historically, cybersecurity leaders have had little visibility into business structure, motivations, and initiatives. Considering that cybersecurity is rooted in technology, shifting to "speaking business cyber risk" is almost like learning a foreign language. This communication gap alone has been enough to keep cybersecurity leaders on the outside looking in at the business.

A holistic picture of cyber risk, supported by financially quantified metrics that can be linked to areas of business impact, empowers security leaders to become business enablers. They can move beyond unprovable ROI budget justifications, speak the language of business, and become trusted advisors who help companies define their risk appetite and identify ways to mitigate risk that are understandable to business leaders.

Lacking financially quantified cyber risks, business leaders and security teams cannot hold productive conversations about security. It is only when cyber risk and its impact to the business are analyzed and this clear communication occurs that business leaders can make informed and intelligent decisions regarding cyber risk and prioritize security investments.

A Tale of Two Cyber Risk Conversations

Picture this: You have a mid-day meeting to discuss cyber risk with your board of directors. The early headlines were dominated by another major breach, so everyone's a bit on edge and imaginations are active.

Eager to both allay fears and convey the great things the team has accomplished over the past quarter, you launch into your presentation:

"We upgraded the SIEM and stopped several DDoS attacks, but are now facing imminent risk from several attack vectors that affect us directly. The Dridex malware has evolved to steal user credentials and data from behind-the-firewall ERP applications. Threat actors are exploiting a vulnerability in the SAP Invoker Servlet, which provides the attacker with full control of the SAP system without requiring a valid SAP user account. As reported in the news this morning, nation-state actors are compromising ERP applications to access highly sensitive information and disrupt critical business processes. Because of outdated IDS and IPS technology, limited network traffic analysis, lack of 2FA, and credentials in the clear, our risk factor is 520. This is red. We have a plan ready to mitigate these risks. To hit the 'go button' on this plan, we will need an additional $400,000."

Even if the funds are approved, which is questionable, the board is likely to feel frustrated at best, and bullied at worst.

What if you were able to elevate the conversation to sound like this?

"We currently report a $48 million cyber risk in the ERP system that is attributed to the type of attack reported in today's news. There is a 35% chance that this attack will be successful in our specific environment. If it were successful, the expected range of loss would be from $15M to $85M. To mitigate this risk, I recommend encrypting the ERP data and implementing two-factor authentication to validate users at sign-on. The costs would be twofold; 1) a price tag of $400,000, and 2) a slight hindrance to system access for authorized employees."

Better? The Board is likely to think so.

Cyber risk analytics empowers conversations like this, and bridges the communications gap between security and the business.

DON'T FORGET

Cyber risk analytics gives security leaders the power to get ahead of cyber risks and prioritize them based on their financial impact to the business.

Chapter 2

The Power of Cyber Risk Analytics

In this chapter

- Understand the nature and components of cyber risk
- Discover the four business-enabling benefits of cyber risk analytics

"Alice: This is impossible.
The Mad Hatter: Only if you believe it is."

– Lewis Carroll

What Is Cyber Risk?

For the purposes of this guide, we define cyber risk as an exposure to negative impacts or losses resulting from inappropriate, unauthorized, or malicious use of technology or systems.

Risk or threat?

Misperceptions fueled by highly publicized incidents and breaches may cause organizations to refer to cyber threats as cyber risks, adding to the confusion over how cyber risk is represented.

A cyber threat is a malicious motivation coupled with a cyber attacker's techniques needed to achieve a mission.

Threats are characterized by the:

☑ Attacker motivation

☑ Actor’s skillset

☑ Techniques used

Depending on its characterization, a threat may or may not be a risk to your environment.

A cyber threat turns into a cyber risk when the cyber threat can be directly mapped to an environmental exposure and potentially do calculable damage to the company.

Components of Cyber Risk

At its core, cyber risk is a function of three components:

1. **The Attacker**. Cybersecurity has the dubious distinction of having an adversary who literally preys on the things that make a business successful, intends to harm the business, and does not play by rules. Because the attacker is a root cause of cyber risk, cyber risk analytics must always account for the attacker.
2. **The Technical Environment**. The technical environment comprises the network topology, vulnerabilities, and active controls. There may be any number of vulnerabilities that permit initial exploit and persistence. In today’s digital environments, this is inevitable, and security teams have the ball in their court to implement controls to mitigate or reduce the risk.
3. **The Business**. It is easy to get distracted by the threat and lose sight of the target. A clear focus on the business assets you are trying to protect is fundamental to effective cyber risk management. It sidesteps the common security problem of boiling the ocean when measuring and managing cyber risk.

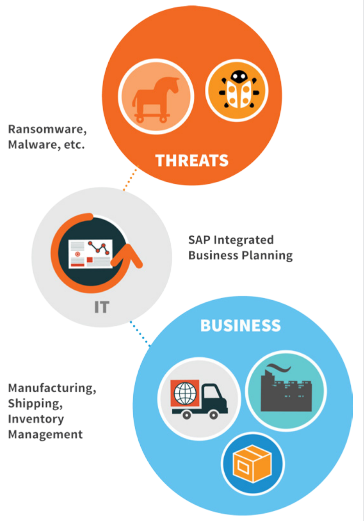
Tracing the Path from Threat to Asset

Attackers target key business applications because that is often ground zero for their reward. They gain access to these applications through the **IT Environment**. IT environments are the engines that drive how the **Business** operates and competes in the marketplace.

Every cyberattack has a motivation and a method. To understand how the attacker reached an asset and what controls were circumvented, it's helpful to view the components of the threat, IT, and business in a linear relationship, from the top down.

Security teams that are able to capture and analyze the data in all of these areas will be able to visualize the connection between the three components, map specific threats to vulnerable IT systems, and directly tie an attack to the business application—and ultimately the business asset—they could potentially affect.

This visibility provides the traceability necessary to not only quantify observed threats in business terms, but also to generate actionable plans for thwarting the revealed risk to the business.



Three Approaches to Cyber Risk Analytics

What is cyber risk analytics? We define it as the discipline of quantifying and monitoring cyber risks so enterprises can make better decisions about how to invest in and deploy cybersecurity defenses. The processes used to assess cyber risks vary, as do their outputs. We will summarize three approaches here.

Assessing risk with grades

One approach to cyber risk analytics is to grade risks through interviews with both technical and business stakeholders, including IT operations and cybersecurity staffs, systems administrators, and line-of-business managers. These stakeholders are asked to assess cyber threats and their potential effect on business operations, and typically to rate them on ordinal scales such as green/yellow/red.

These ratings can be an excellent *starting point* for risk assessment, but they also have serious drawbacks, including subjectivity, inconsistency, and limited guidance for prioritizing cybersecurity investments. We will examine the pros and cons of ordinal scales a little more in Chapter 3.

Assessing risk at a technical level

Some organizations gather and analyze large amounts of intelligence about currently active cyber threats and tie those back to known vulnerabilities in the enterprise's network and systems. The outputs usually include prioritized lists of critical weaknesses that are tailored to the enterprise, based on its industry and the specifics of its computing infrastructure.

This approach can be useful for identifying probable risks in cybersecurity defenses. However, this laser focus on the technical issues loses all business context and makes it challenging to communicate risks to business stakeholders.

Assessing risk with quantitative business metrics

A third approach to cyber risk analytics, the one we are advocating in this guide, involves understanding the enterprise's business and technical environments and applying intelligence on the attacker to quantify potential losses.

This involves:

- ☑ Identifying critical business assets, processes, and their value to model the business environment.
- ☑ Understanding IT systems supporting and protecting the critical business assets and processes in order to model the technical environment.
- ☑ Utilizing threat intelligence to determine the types of attacks most likely to affect the enterprise.
- ☑ Based on the models of the enterprise's business and technical environments, estimating the likelihood that each attack type will succeed and the resulting loss.

The output of this process is two critical metrics for each attack type: 1) probability of loss and 2) a computed loss.

This modeling/quantifying process bridges the gap between IT exposures and potential business impacts. The two key metrics allow the IT organization to talk to executives and business managers in dollars and probabilities, a language they understand. The metrics also enable the enterprise to compare the cost of proposed cybersecurity defenses with the probable reduction in losses.

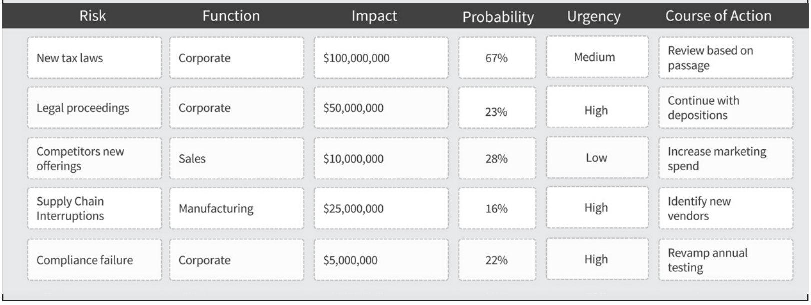
We will discuss this process and the two key metrics in detail in Chapter 4.

Risk-informed Management and the Risk Register

Ultimately, the promise of cyber risk analytics is to fuel risk-informed management within the business. This may sound highly visionary and unattainable. The reality is, however, that much of the groundwork to manage cyber risk already exists. Organizations already employ frameworks and metrics to monitor risks on a regular basis. The most commonly used mechanism for centralizing and communicating risk is the risk register.

A risk register is a key tool used by risk management programs to capture, communicate, and manage risks. It serves as a living document that departments use to log and communicate their top risks as they shift and change over time. The power of the risk register becomes apparent when C-level executives and boards see top risks laid out side-by-side, measured in the same units, and described in the same language—dollars. Managing risks across the enterprise in this way empowers stakeholders to make contextual decisions and focus on the company's top priorities.

When done right, cyber risk analytics provides the dollar figures, probabilities, and prioritization that allow cyber risks to be compared and managed like other classes of key business risks.



Risk	Function	Impact	Probability	Urgency	Course of Action
New tax laws	Corporate	$100,000,000	67%	Medium	Review based on passage
Legal proceedings	Corporate	$50,000,000	23%	High	Continue with depositions
Competitors new offerings	Sales	$10,000,000	28%	Low	Increase marketing spend
Supply Chain Interruptions	Manufacturing	$25,000,000	16%	High	Identify new vendors
Compliance failure	Corporate	$5,000,000	22%	High	Revamp annual testing

DON'T FORGET

The risk register is an ideal tool for cyber risk management because it enables you to: 1) record, 2) prioritize, and 3) communicate risks across all departments.

Business Benefits of Cyber Risk Analytics

Business Enabler #1: Protect Business Value

Cyberattacks invariably result in operational impacts. The target company might redirect resources to deal with the attack, or the attack itself might halt operations. The ability of cyber risk analytics to proactively prioritize high-profile exposures can diminish the cost of—if not totally avoid—substantial impacts.

Business Enabler #2: Prioritize and Optimize Investment

Cyber risk analytics transforms a reactive technical conversation about threats into a proactive business dialogue about financial exposure stemming from cyber risk. Armed with an understanding of validated cyber exposure, security teams can answer the following questions:

- Where's my risk and what is causing it?
- What is the probability the risk will occur?
- How severe is the risk?
- How urgent is the risk?
- What should I do?

Companies that use analytics well are able to make their businesses run faster, reduce their losses, and more intelligently manage their expenses for technology, services, and cyber insurance. These are real returns to the business.

Business Enabler #3: Empower a Risk Intelligence Culture

In modern-day businesses, responsibilities and actions are spread across departments to empower agility and performance. Business functions like sales, marketing, and accounting test out new technologies on a continual basis. Each autonomous decision they make to change processes or technologies, or to connect to new systems or to a new partner, is likely to generate a cybersecurity risk.

Using cyber risk analytics across the enterprise sheds light on the cyber risk impact of such technology decisions. By creating a culture of risk intelligence, business leaders can continue to take autonomous actions while keeping the security of the business in mind.

Business Enabler #4: Drive Informed, Defensible Decisions

From executive leadership (which answers to regulators, customers, and investors) to security leadership (which reports to executive leadership and the Board) down to the security operations team (who are accountable to security leadership), decisions as to what to do, what actions to take, and where to invest time and money are being made on a daily basis.

Cyber risk analytics directly ties cybersecurity expenditures to core business functions. By providing logical plans and actions that boards and C-level executives can implement and measure, cyber risk analytics empowers companies to take smart risks that are defensible in terms of intelligent resource prioritization and investment decisions.

More on defensibility

With cyber threats continuing to proliferate, there is an increasing need to make defensible decisions on what to do, what not to do, what actions to take or avoid, and where to invest time and money. Defensibility means stakeholders would agree that the best decision was made with the information available at the time. Unfavorable outcomes, such as a data breach, may trigger a review of defensibility, but bad outcomes do not equate to lack of defensibility.

Multiple Layers of Defensibility

Defensibility is a concept that has multiple layers, each of which has a defender, an area of responsibility, and a stakeholder. At the core, the security team is responsible for securing the network and business assets. The security team members are accountable to security leadership for their decisions and actions. Similarly, security leadership is responsible for defending the security program, initiatives, and budget, and is accountable to the Board and C-level executives. Lastly, the Board and executive leadership are responsible for decisions regarding cyber risk management, and are accountable to customers, partners, investors, regulators, and M&A partners.

Each stakeholder layer needs to know that carefully considered decisions are being made to appropriately defend the enterprise. Thumb in the air, or reactionary, decision making leads to an indefensible approach to managing cyber risk. A better strategy is to implement a consistent cyber risk management program powered by cyber risk analytics to support informed, defensible decisions.

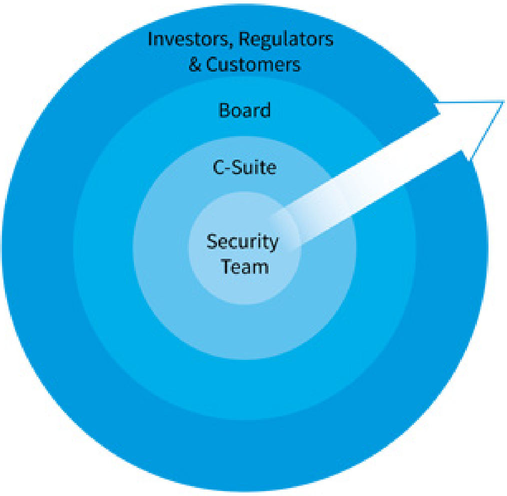


Figure 2-1: Multiple layers of defensibility

Chapter 3

Why You're Doing Cyber Risk Measurement Wrong

In this chapter

- Understand why current methods fall short
- Learn the four common mistakes in measuring cyber risk
- Discover combat techniques to help guide your efforts

"You can't manage what you don't measure."

– W. Edward Deming

The ability to quantify cyber risk provides a significant advantage when implementing a cybersecurity strategy and prioritizing investments. However, measuring cyber risk within a corporate environment has proven exceptionally difficult.

The most common shortcomings for companies pursuing cyber risk as a business enabler are:

- ☑ They are missing large segments of data and processes from their cyber risk approach.
- ☑ They are failing to advance the exercise into the business arena so security decisions can be made within an organizational context.

Current Methods Fall Short

For organizations stepping up to the challenge of measuring cyber risk, the first stop is often ordinal scales or Monte Carlo simulations. While these risk analysis methods are fast and easy and enable a basic understanding of risk, they fail to quantify cyber risk in ways that make sense to the business, and fail to support rigorous decision making.

Ordinal scales

Qualitative risk analysis is the process of using ordinal rating scales (1-5 or red/yellow/green) to plot risks based on their frequency (likelihood of occurrence) and magnitude (impact of loss). With these scales, organizations can visually represent the relative severity of the various risks they face. While qualitative risk analysis is efficient, suited to quick decisions, and easy to communicate, it is insufficient for leaders to make intelligent and timely decisions. Ordinal scales are:

- ☑ Highly subjective, error prone, and open to bias
- ☑ Inconsistent in analysis and ambiguous in meaning (What does “red/high” really mean?)
- ☑ Difficult to prioritize (Which red is the “reddest”?)

Monte Carlo simulations

Some organizations model cyber risk based on Monte Carlo simulations. Monte Carlo is a computerized, mathematical simulation technique that generates estimates for complex problems where there is significant uncertainty. It essentially simulates situations by repeatedly flipping a coin to calculate probabilities of various outcomes.

Monte Carlo simulation is a step in the right direction toward greater rigor in calculating cyber risk, as it injects math into what is otherwise a subjective scenario.

There are, however, several drawbacks:

- ☑ The results are not specific to your organization.
- ☑ The simulation does not take into account the IT environment, the vulnerabilities present, and, more important, the security controls in place.
- ☑ The model suggests a predictability of behavior that doesn't exist when dealing with the element of a persistent human hacker.

The risk calculated is theoretical and only loosely represents reality. Savvy business executives will thus stop short of basing important decisions—and staking their professional credibility—on the outcomes of Monte Carlo simulations.

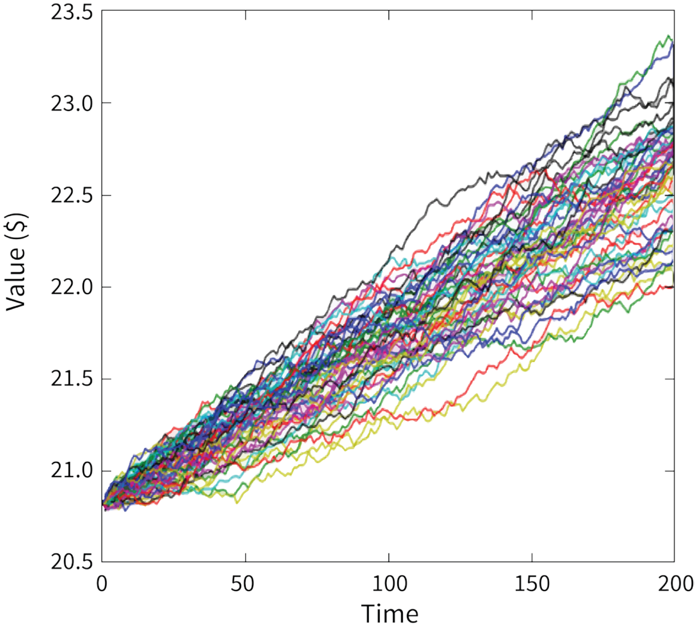


Figure 3-1: Simulated paths of an asset's value using Monte Carlo

Four Common Mistakes in Measuring Cyber Risk

Informed leaders are realizing that it is time for a fundamental rethink of how cyber risk is measured, quantified, and understood within their firms. Undertaking such an exercise is no easy feat. Four common pitfalls to avoid are:

1. Thinking it cannot be done
2. Boiling the ocean with a match
3. Using unrelated data
4. Relying on stale data

For each pitfall, we also offer some combat techniques to help ensure your efforts are successful.

Thinking it cannot be done

When it comes to quantifying cyber risk, many companies never get started. They remain smothered by the flow of alerts or become paralyzed by doubts about their ability to quantify cyber risk. Unfortunately, this doubt is sometimes reinforced by industry analysts repeating outdated guidance against using quantitative risk assessments in favor of stories to demonstrate the likelihood and impact of risk. With cyber risk analytics still on the launch pad at most companies, such thinking is standing in the way of progress.

Combat technique

Measuring cyber risk is neither simple nor easy, but it is possible. Learn more about how to get a handle on cyber risk—there is a growing body of resources out there. Enlist an internal champion (or be one!) and create a small, internal project with believers who are willing to tackle a reasonable project to show that it can be done. Check out the next chapter, "Cyber Risk: What to Measure, Where to Start," for a practical discussion on how to get started.

ON THE WEB

Want to learn more? Download the Nehemiah Security ebook, Cyber as a Business Enabler.

Boiling the ocean with a match

The security department arguably manages more data than any other department within the organization. With so much data available, there is a tendency to want to dive in and see what gems of intelligence you can glean. Without direction, you either end up working with the wrong data or getting bogged down in too much data. Either way, the result is often becoming overwhelmed by the vastness.

Combat technique

Start with a small part of the business where you have visibility into the business and IT operations. Trace the path to the valuable data created, stored, and managed by business processes. Identify the systems responsible for making that business process run, and map out security controls and known vulnerabilities in those areas.

Using unrelated data

You've been there. A headline-grabbing breach hits the media. The next day every CISO gets to field the question from their board, "Are we susceptible to this attack?" It's a reasonable question, especially within companies operating in the same industry as the one that was compromised. However, even companies in the same industry that operate very similarly will look different from an IT and cyber defense standpoint. This makes each investigation unique for each company.

Possessing limited data about the breach—and lacking cyber risk analytics—companies often use any available information to assess the situation and gauge the degree to which they are susceptible to the headline attack. The warning here is to avoid over-relying on industry data, or scenarios, simply because they share a few commonalities.

Combat technique

Every company is unique in business model, IT environment, business applications, and attack profile and cyber defenses. The combat technique is to gain control by establishing a cyber risk profile specific to your company. Armed with the knowledge of your own cyber risk, you'll have a ready answer when questioned about how susceptible the company is to a particular attack.

Will Lowe's Be Breached?

If Home Depot suffers a breach that loses millions of records and costs tens of millions of dollars, is Lowe's also staring down the barrel of a similar attack? Not necessarily. While companies in the same industry can be subjected to similar attack threats, every company is unique based on its IT and business environment fingerprint.

Both firms store customer data and conduct a high volume of online transactions, data that would be valuable to a hacker. While both are in the same industry and have exposure to similar loss types, it doesn't mean that Lowe's is automatically subject to the same attack. Lowe's best bet is to create a cyber risk profile that lets them know if their particular house is on fire—or not.

Relying on stale data

One of the biggest challenges—and one of the biggest surprises to leadership—is that the data used in the analysis of cyber risk may be quite old. For example, some firms run vulnerability reports once a month, or less frequently. Once leadership has visibility into cyber risk, the inclination is to mitigate the threat, recalculate risk, and immediately see to what degree it has been reduced. Even after mitigation, a refresh of the cyber risk may not yield a change in the risk score if the input data is not also updated.

Some firms rely on third-party consulting firms to assess and quantify their risks. The upside is the ability to leverage leading professionals. The downsides include scope limitations, cost, and—again—timeliness. Because the data is stale, the report is essentially out of date when it's delivered.

Combat technique

The problem is the disconnect between the dynamic nature of the shifting IT, business, and attack environments and vulnerability scan cycles. As a first step, be clear about how often data is refreshed and whether the scan cycle meets the company's needs. When timeliness becomes critical, there is a need to move to a software solution that can accommodate real-time analysis and decision-making.

TIP

Increase communication with executive leadership to set expectations on the relationship between data refresh cycles, risk mitigation, and cyber risk scores.

Chapter 4

Cyber Risk: What to Measure, Where to Start

In this chapter

- Learn what it takes to get started in measuring cyber risk
- Understand three elements instrumental in measuring cyber risk
- Get an overview of the cyber risk measurement process

"The journey of a thousand miles begins with one step."

– Lao Tzu

For many organizations, monitoring and managing cyber risk is new. The good news for security executives leading the charge to quantify cyber risk is that the organization is accustomed to managing other risks throughout the company. By partnering with the organization, security leaders can take one step at a time to build out the cyber risk program.

Let's Get Practical: Where Do You Start?

To get started with cyber risk analytics, you should:

☑ Find a champion

☑ Focus on business priorities

Find a champion

A critical component to introducing cyber risk analytics to the business is a devoted champion who:

- ☑ Recognizes the need for cyber risk analytics
- ☑ Understands how cyber risk analytics can drive business decisions
- ☑ Is willing/able to jumpstart a project focused on one or two priorities of the business

The road to implementing change can be winding and bumpy; the role of the champion, demanding. To be successful, the champion must be:

- ☑ A leader who has the ear and trust of executive management and is empowered to facilitate action and investment
- ☑ An effective networker able to make connections, gain cooperation across functions and departments, and capture the necessary data
- ☑ An inquisitive, tireless learner who never stops testing their own calculations, assumptions, and conclusions

Focus on business priorities

Start with one to three key business applications to which you have access and visibility. We recommend prioritizing:

- ☑ Revenue-generating business applications
- ☑ Applications that hold critical data, such as customer information
- ☑ Areas that historically have caused the business significant loss (collaborate with leaders, such as the CFO, to identify areas of concern)

The key to success and survival is to start small, and then build on your success by expanding the analysis to additional business processes and applications.

Two Critical Metrics

When building out a cyber risk analytics program, there are two critical metrics that come into play. These key metrics are: 1) probability of loss and 2) computed loss.

Together, these metrics answer the questions: “Where is the risk?” and “What could be lost?” Armed with these answers, leaders can wrap their arms around the full scope of cyber risk.

Probability of loss

Determinants for probability of loss are:

- ☑ **Frequency of occurrence**: the number of times a company is likely to find itself in the crosshairs of an attacker.
- ☑ **Probability of success**: the probability an attack will successfully navigate the IT environment to impact the targeted business asset.

Once a connection between the attacker, their methods, the IT environment, and the business environment is established, cyber risk analytics can be used to analyze attacker methods and motivations and all probable paths of attack against the IT environment to determine probability of loss.

Understanding Probability of Loss

Cyber risk scenarios with a high probability of loss have vulnerabilities that attackers can use to reach their reward, and gaps in controls to block the attack path. Conversely, scenarios with a low probability of loss have controls and processes in place to block and/or mitigate an attack. Let's look at some examples.

High Probability of Loss

A back door on a compromised server allows the attacker to gain entry and establish command and control. Because the system admin has not changed his password, the default admin password allows the attacker to gain admin privileges and explore the network undetected. Lateral movement reveals 50 million unencrypted customer records, which the attacker exfiltrates undetected.

Low Probability of Loss

An employee clicks on a well-crafted phishing email, allowing malware to infect the endpoint. Automated detection and response technology recognizes aberrant activity on the endpoint. Automated workflow processes isolate the infected endpoint for remediation. The attacker is stopped dead in his tracks.

TIP

Computing probability of loss for multiple attack types can take a lot of brain power and staff time. This is where the power of an automated cyber risk analytics tool starts to become important.

Computed loss

Computed loss is lost asset value over time. It tells the business story of cyber risk and answers the question: "How much is at risk?"

Similar to probability of loss calculations, cyber risk analytics will analyze attacker methods and motivations and probable paths of attack against the IT environment *and also the business environment* to determine computed loss. Here, the analysis considers the profile of the business and possible impacts, such as amount of online transactions, number of customer records stored, etc.

Not all cyber risks are created equal. Some attacks, such as a denial of service (DoS) attack, can trigger a $5M loss within hours. Other attacks might require months to incur $10M of loss. Further, some attacks will trigger loss events such as data destruction, while others will cause data compromise (think privacy loss).

Figure 4-1 and Figure 4-2 compare the impacts of two attack types and illustrate the importance of understanding all of these metrics.

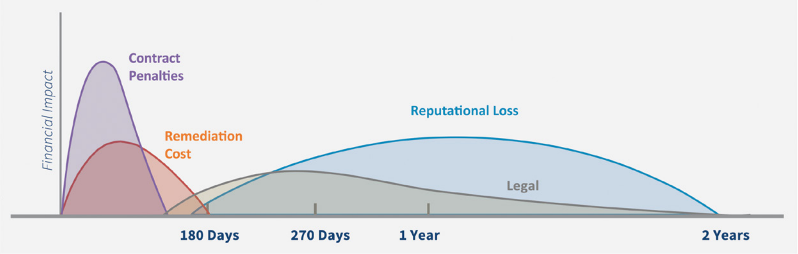


Figure 4-1: Impact of a data breach attack over time

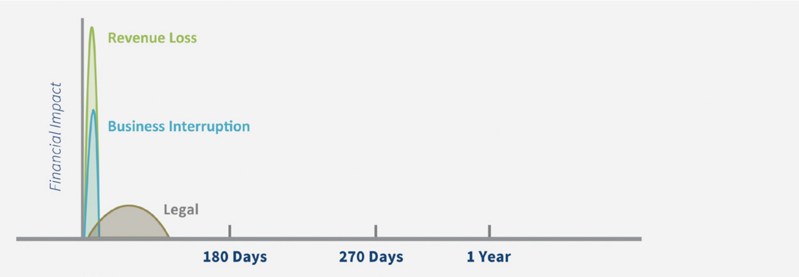


Figure 4-2: Impact of a DDoS attack over time

Three Sources of Data

Before gathering data, remember the four dimensions of cyber risk you want to deliver insight on:

1. What is the likelihood that the risk will occur?
2. Where is your vulnerability to the risk?
3. How severe is the risk?
4. How pressing is the risk?

To get answers to these questions, it is imperative to identify and aggregate the right data sources.

Calculating cyber risk requires tapping into three dynamic sources of data: 1) attackers, 2) the IT environment, and 3) the business landscape.

Attackers

It's impossible to create a full picture of the risk your company faces without understanding how potential attackers work in general and, more important, why they may be interested in your organization in particular. Attackers are motivated in different ways: some by financial gain, others by espionage, and still others by ideology.

Different enterprises, and even different units within the same enterprise, will be more or less vulnerable to the motivations of a potential attacker. It's important for a company or line of business to look at itself from the attacker's perspective and get clarity on the biggest exposures from the standpoint of an attacker's specific motivation. Once you understand motives, you can start to identify the methods an attacker might use to navigate your corporate network and achieve their goal.

The IT environment

Three elements make up every IT environment:

- ☑ Network topology
- ☑ Vulnerabilities
- ☑ Controls

Because the IT environment is constantly changing, the typical cybersecurity mindset is to want to maintain a constantly updated network map. While a network topology is vital to minimize blind spots, what's more important is a keen sense of the attacker's potential methods for accessing and navigating the network.

This approach will narrow down the universe of vulnerabilities to just the ones that an attacker could exploit to impact the business. However, all the vulnerabilities in the world are useless to an attacker if controls are activated to stop or deter the threat. An attacker can be hyper-motivated and have a well-planned method to gain access, but if effective controls are in place surrounding the business asset, the attacker is not going to get anywhere.

The business landscape

Within an enterprise, all transactions, operations, goods, services, business intelligence, and analytics rely on a set of business applications that support the company's functions.

Examples of these business applications include enterprise resource planning (ERP), such as NetSuite, or customer relationship management (CRM), such as Salesforce.com. It's helpful to think of these applications as the heartbeat of the business that relies on underlying IT infrastructure to access and transmit data.

Each application is associated with a finite and knowable set of business impacts that could be incurred through attacks on that application. Two components important in identifying the type of losses from attacks to any given application are:

- ☑ Type of business process handled by the application (sales cycle, accounts payable, inventory management, etc.)
- ☑ Type of business asset stored by the application (financials, customer records, intellectual property, contracts etc.)

If applications are impacted, the connected business process is also impacted, stored assets are placed at risk, and costs quickly mount.

The business environment, therefore, adds the financial context needed to calculate the amount of a potential loss. It also establishes the boundaries for the nature of a potential loss, such as lost revenue from system downtime, exposure of confidential records, or theft of intellectual property.

Overview of the Cyber Risk Quantification Process

There are four steps to quantifying cyber risks and two prerequisites: modeling the business and modeling the supporting IT environment. Let's look at these prerequisites first.

Modeling the business environment

Stage 1: Diagram the organization's structure to create a profile of business units and their related processes. This can be a fairly straightforward exercise to map the landscape and start the conversation between security and business stakeholders.

Stage 2: Select the business processes you want to focus on.

Stage 3: Develop a profile for each selected business process that includes:

- ☑ The business process profile (geography, supporting offices, regulatory and compliance requirements)
- ☑ Business assets and their values tied to each process (annual revenue, number and type of data records, business disruption costs, contracts)
- ☑ Critical business applications that support the company's assets

TIP

Start by sitting with a finance or operational executive to identify the crown jewels of the organization and map out the business processes in which they reside.

Modeling the supporting IT environment

After you model the business environment, the next prerequisite is to model the IT environment that supports the selected business applications.

Stage 1: Document the IT assets tied to the previously targeted applications, along with any vulnerabilities and exposures affecting the IT assets and the applications.

Stage 2: Identify controls in place that have the capability to neutralize some or all of the vulnerabilities.

TECH TALK

Active Directory (AD), simple network management protocol (SNMP) logs, vulnerability scans, and configuration management databases (CMDB) are good sources to get started in assembling this information.

Cyber risk quantification in four steps

By running through these two prerequisite exercises, you can create a blueprint that reflects financial values and location of business assets, as well as location of vulnerabilities and surrounding controls. This blueprint will serve as the foundation for launching into the following four steps of calculations:

Step 1: Identify the types of attacks most likely to affect your company. This intelligence is commonly found in threat intelligence feeds that monitor and aggregate historical data on attacks. Knowledge about the most likely attacks will allow you to estimate the **frequency of occurrence.**

Step 2: For each type of attack that is likely to target your company, determine the probability that it will reach a critical business asset. This becomes an analysis of attacker tactics, techniques, and procedures (TTPs) mapped onto existing vulnerabilities. Overlay that with the controls in place to deter attacks and you are left with a complex game of capture the flag with your business asset as the prize. This analysis allows you to estimate the **probability of success.**

Step 3: Once you have determined which attacks can reach which business assets, it becomes a matter of determining whether the attacker can do damage to that asset and, if so, what type of damage. For example, consider that even if a DoS attack can disrupt a server storing PII data, it's irrelevant. The business will incur minimal to no damage in such a scenario. Conversely, should ransomware target that same server, the business will incur damage as a result of the attack.

Step 4: The final step is to compute how severe the loss will be if incurred by the business. Remember to take into account the attacker and how different attack techniques can trigger different impacts depending on the asset. This gives you the **computed loss**.

TECH TALK

We recommend modeling computed losses using an attack-cost model that uses historical, proven data points, and case studies. These user data, attack strands, and risk intelligence components will ensure an accurate number for **computed loss**.

The power of automation

Calculating the loss types and impact across all four dimensions of cyber risk, for every business process, running in every key business application, for every threat the organization faces is a daunting, multi-dimensional challenge. Some would say it's impossible to do.

If it weren't for automation, we might agree. Automated cyber risk analytics solutions use between hundreds and thousands of sophisticated algorithms to compute the business impacts of cyberattacks.

By distilling a hyper-dynamic, multidimensional problem (times three for the three components of cyber risk: attacker, IT environment, and business environment) down to meaningful numbers presented in the language of business—dollars and risk—cyber risk analytics provides a foundation for meaningful dialogue.

Chapter 5

Making Decisions Using Cyber Risk Analytics

In this chapter

- Discover the power of adding cyber risks to the risk register
- Understand how to frame security conversations for business context
- Learn four risk response strategies

"Plans are nothing; planning is everything."

– Dwight D. Eisenhower

No organization has enough resources to completely eliminate cyber risks. This places incredible importance on making the right choices regarding risk response strategies. The time has arrived for security leaders to step up as business leaders who communicate and strategize about cyber risk in the context of the business.

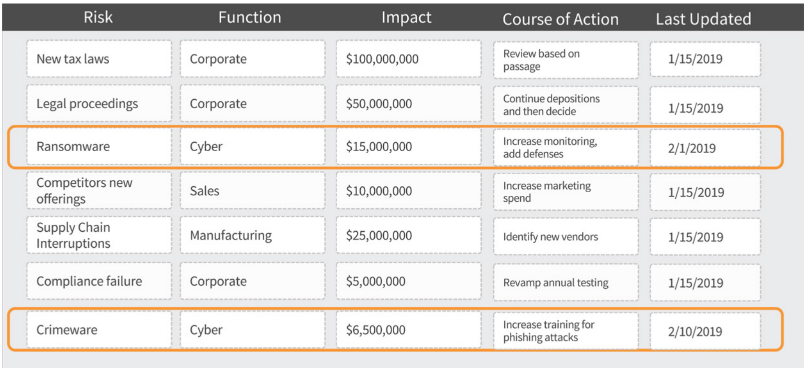
Adding Cyber Risk to the Risk Register

With cyber risk management still making its way into boardrooms, a common business language shared by security and business leaders is in the early stages. Stakeholders seek clarity with regard to cyber risk and its business impact, but information gaps lead them to draw unsupported conclusions and make uninformed decisions. It's up to security leaders to both translate cyber risk into a language that all stakeholders can understand and fill in the gaps in data.

The good news is that money is the universal business language. More good news is that the security team doesn't need to reinvent the wheel regarding risk management. Most companies already use some form of a risk management tool, such as a risk register, to capture, communicate, and manage business risks. As introduced in Chapter 2, the risk register serves as a living document that the organization uses to log and update its top risks. Because the risk register, or a similar risk management tool, represents the impact of risks in dollars, it ensures all business units are speaking the same language.

Putting a dollar value on cyber risks so they can be included in the risk register has important ramifications. By using this existing and well-established tool as the starting point for communicating cyber risk, security leaders can bridge the gap between cybersecurity and the rest of the business and earn a seat at the boardroom table.

The power of the risk register becomes apparent when leaders see top risks laid out side-by-side and measured in the same units and language. Managing risks across the enterprise in this manner empowers quicker decision making and enforces focus on the company's top priorities.



Risk	Function	Impact	Course of Action	Last Updated
New tax laws	Corporate	$100,000,000	Review based on passage	1/15/2019
Legal proceedings	Corporate	$50,000,000	Continue depositions and then decide	1/15/2019
Ransomware	Cyber	$15,000,000	Increase monitoring, add defenses	2/1/2019
Competitors new offerings	Sales	$10,000,000	Increase marketing spend	1/15/2019
Supply Chain Interruptions	Manufacturing	$25,000,000	Identify new vendors	1/15/2019
Compliance failure	Corporate	$5,000,000	Revamp annual testing	1/15/2019
Crimeware	Cyber	$6,500,000	Increase training for phishing attacks	2/10/2019

Figure 5-1: Cyber risks represented on the risk register

Communicating Cyber Risk

To manage cyber risk, security leaders must interact with a suite of stakeholders across the organization. While identifying the right contacts is important, it's equally critical to find common ground with all these players.

To prevent jargon from creeping into the discussion and causing confusion, it's vital to emphasize business impact. Technology is a source of the cyber risk problem and the way it will be mitigated. The business impact is why it matters. Frame conversations with challenges and objectives the business understands and monitors.

Frame the Conversation for Business Context

When communicating cyber risk, frame the conversation in terms of business impact. Four objectives to highlight in each conversation are:

Availability: Keep business processes running, and recover from failures within acceptable timeframes

Access: Provide information to the right people while keeping it away from the wrong people

Accuracy: Ensure information is correct, timely, and complete

Agility: Change business processes with acceptable cost and speed

A best practice is to integrate the relevant objectives from this list in every conversation to maintain the business context, which empowers stakeholders to prioritize the risk and decide how to handle it. With this business context, security conversations can sound like this: "We have 25,000 PCI records vulnerable to a crimeware attack. Projected loss exposure is $5 million, and there is a 20% chance of loss within the next 14 days. To mitigate this risk, I recommend encrypting the data. The costs would be twofold; 1) price tag is $150,000, and 2) ease of access for employees would be hindered."

Now THIS is a conversation that empowers stakeholders to strategize effectively, knowing the full scope of business impacts!

DON'T FORGET

Dollar figures provide a common point of reference when conducting risk assessments. When discussing security priorities with executive leadership, you should expect risk to be at the center of the conversation.

What Stakeholders Want to Know About Cyber Exposure

By putting a dollar amount on cyber risk, security leaders expand the number of stakeholders who care about how cyber risk impacts the business. Here's a look at the players and how to address their concerns.

What do you mean we have a $70M exposure?
How is this going to affect the company's risk appetite?
Is this going to put us in the headlines?
This should be flowing through my department.
What controls do we have to protect the data?
I'm trying to do my job and you're slowing me down.

Chief Executive Officer. The CEO must choose between conflicting business priorities and will want to know how cyber risk impacts business operations. Provide timely, financially quantified intelligence the CEO can weigh against other initiatives, along with options to manage this risk.

Chief Financial Officer. CFOs evaluate technology spend in the form of programs that project future spending needs and calculate ROI. Show them how proactive investment in cybersecurity resources can remain aligned with business initiatives and get ahead of developing risks.

Chief Risk Officer. The CRO keeps a finger on the pulse of risks across the enterprise. Deliver regular updates on cyber risks so the CRO can integrate them into the risk register to support further discussion and investment.

Chief Information Officer. The CIO drives technology integration across the enterprise and between the company and its trading partners, thus connecting the goals of the business to the IT and data strategy. Collaborate with the CIO to integrate cyber security into enterprise risk discussions in order to review additional risks and minimize exposures.

Line of Business Owners. Business owners must understand that cybersecurity is a critical element of their success and accept a share of the responsibility for cyber risk. Laying out options for handling cyber risk gives them flexibility to choose according to what's best for the business.

Now That We Have Your Attention: What Are the Options?

Including cyber risks on the risk register elevates the conversation and prompts tough questions from the entire organization: “Who owns this cyber risk?” “How should it be handled?” “What is our cyber risk appetite?”

The good news is that while such conversations are new territory for security leaders, most organizations already have an understanding of their risk appetite and a framework for responding to risk.

Risk response: what does risk appetite have to do with it?

Risk appetite is the risk an organization is willing to accept as part of normal business operations. Risk tolerance is the amount of risk above the risk appetite that might be acceptable for a high-value initiative. Stakeholders don’t always grasp how much technology-related risk they are exposed to or whether the cyber risk within their operations falls within the boundaries of the company’s risk appetite. Knowing how much cyber risk the company is willing to accept, as well as tolerate, is therefore fundamental to determining an appropriate risk response strategy.

Risk response strategies

While other considerations may come into play, risk appetite is the chief measuring stick you and the risk owner will use to determine the right response strategy. Four risk response options are:

☑ Accept the risk

☑ Mitigate the problem

☑ Transfer the risk

☑ Avoid the risk

Accept the risk

One option is to accept the risk and do nothing. This option is often used for risks that carry a low probability of occurring or would have a low impact if they did occur. This is a viable option where the cost of mitigation or insurance would be greater over time than the losses sustained.

Mitigate the problem

If the threat is determined to be high priority and action is needed to address the risk, one option is to execute a risk mitigation plan, including enacting proper controls to reduce likelihood of impact.

Transfer the risk

One option is to transfer the risk. In doing so, you don't eliminate or reduce the risk, but rather delegate it to the internal business owner or external trading partner best able and most motivated to properly manage it. Insurance also transfers risk, but is not a silver bullet. It doesn't reduce the risk of attack, but provides a safety net if one occurs.

Avoid the risk

When considering new strategic initiatives, including cyber risks into the discussion is critical. If the risks exceed a company's risk appetite, they can choose to avoid the risk by selecting a different initiative.

A Look at Risk Responses

Responses should be appropriate to the level of a threat or opportunity and be developed with the security team and business stakeholders.

Let's presume the probability of a threat succeeding is low. The expected loss is $100,000, but it would cost $250,000 to eliminate the risk. The firm may decide to accept the risk due to the combination of low probability and high mitigation costs. If the probability that the threat will succeed is higher, but it's tied to a high-value product launch, for example, the firm may decide to tolerate the risk, but transfer it to the business owner to capture the costs in their budget. However, if the risk presents a $750,000 threat with a high probability of occurring, the firm may wish to allocate funds to mitigate the vulnerability or obtain insurance to cover any losses.

Chapter 6

Mission: Possible

In this chapter

- Find out how to set yourself up for success in computing cyber risk
- Review a questionnaire of items to address in getting started
- See a roadmap of how to structure your journey to delivering full transparency around cyber risk

"Start by doing what's necessary; then do what's possible; and suddenly you are doing the impossible."

– St. Francis of Assisi

While quantifying cyber risk is a priority for a growing number of enterprises, it is also extremely challenging. Companies are accustomed to managing their business through risk-informed decision making. Up to now, cybersecurity has been unable to join in because it has been too hard to translate technology-related risks into financial metrics. Quantifying cyber risk is possible with cyber risk analytics. Armed with the capability to measure and analyze cyber risk, security teams can now integrate with the way the rest of the business operates.

Become a Cyber Risk Champion

Organizations are ready to benefit from the promise of cyber risk analytics. It takes just one person with a vision of what's possible and a willingness to take the initiative in introducing cyber risk analytics to the business.

Your mission, should you choose to accept it, is to don the mantle of a cyber risk champion and jumpstart an initiative that will:

- ☑ Deliver cyber risk clarity that includes placing dollar values on the potential impact to the organization as a whole, as well as functional impacts on the lines of business
- ☑ Drive risk-informed, defensible security decision making across the organization
- ☑ Prioritize investment decisions to mitigate risk exposures and investment decisions

Mission Possible: When You Can Quantify Cyber Risk

When you understand cyber risk and are able to quantify it in dollar terms, you will be able to:

- Communicate more effectively with executive leadership and the board of directors about cyber risk
- Prioritize security initiatives
- Justify your current budget—as well as persuade leadership to increase it
- Do more with existing resources—and determine where to assign team members so they can have the maximum impact

Set Yourself Up for Success

Implementing change can be demanding. And while the efforts of the champion will be paramount, it is nearly impossible to go it alone. Before you launch the cyber risk quantification project, be sure to:

- ☑ Bring the security team on board by sharing the vision of how cyber risk analytics will benefit their day-to-day lives
- ☑ Educate your executives to ensure they embrace the value of the program and commit to supporting it

- ☑ Engage with executives and business managers so they understand how to contribute to the effort and how it will benefit their organizations
- ☑ Assess where you are today (see the questionnaire below)

Launch Checklist

Here's a list of questions to answer before getting started.

- ☐ Are you empowered by executive sponsorship?
- ☐ Is your security team on board with the cyber risk analytics initiative?
- ☐ Do you have interdepartmental access?
- ☐ Do you have all of your data accessible in one place?
- ☐ Are there any gaps in your data?
- ☐ Is your data up to date?
- ☐ Are you able to run sophisticated calculations (ideally in an automated manner)?

Automate with a cyber risk analytics tool

Calculating cyber risk requires tapping into three data sources to get information about:

- ☑ The attackers' motives and methods
- ☑ Vulnerabilities and controls in the infrastructure
- ☑ The company's applications, processes, and data

Computing the business impact of cyber risk across all of its dimensions, for every business process and application, and for every threat the company faces is a multi-dimensional challenge. Automate the process either by creating your own tools or by investigating cyber risk analytics solutions already on the market.

Your journey to cyber risk analytics leadership

Each organization's journey to cyber risk analytics is different, but they all begin with planning and include similar milestones.

Here is a roadmap of how to structure your journey to delivering full transparency around cyber risk.

1. Begin with a small project—ideally a sliver of the organization where you have visibility and access. Be sure to publicize your success and results within the organization.
2. Learn from this small project to refine the methodology and tools.
3. Talk with other people in the company who are already involved with risk management to learn from their experiences. Integrate your initiative with what's already in motion to avoid surprises and mature your program.
4. Build on initial success by expanding the analysis to other business applications and functions.
5. Be a thought leader. Share your vision and success with your corporate colleagues and security professionals outside the company who are trying to measure their risk.

Mission Accomplished

When you are introduced to what's possible, it is hard to go back to the way things were. Cyber risk analytics fits this description perfectly.

It has emerged to fill the need for a methodology that can quickly, easily, and accurately measure cyber risk from a business perspective and enable well-informed, defensible decision making.

By becoming a cyber risk champion you can take the lead on determining how much your current and future security investments can reduce risk and communicate that information in a language that everyone understands.

Learn how cyber risk analytics dramatically increases the ability to financially quantify the business impact of cyber risk and make better investments in security.

Security leaders must justify their programs and spend to multiple stakeholders. Few, however, would profess a high level of confidence that they always deploy resources to the biggest threats facing the company. Fewer still would say they effectively communicate cyber risk to executive leadership. If you are involved in measuring, communicating, and managing cyber risk, this book is for you.

- Understanding the case for cyber risk analytics — review the challenges of measuring and communicating cyber risk
- Learning the power of cyber risk analytics — explore the components of cyber risk and the business benefits of cyber risk analytics
- Realizing why you're measuring cyber risk wrong — learn common mistakes in measuring cyber risk
- Getting started in measuring cyber risk — get an overview of the cyber risk measurement process
- Making decisions using cyber risk analytics — discover the power of adding cyber risks to the risk register
- Becoming a cyber risk champion — find out how to set yourself (and your company) up for success in measuring cyber risk

About the Authors

Suzanne Porter-Kuchay is a high-tech industry veteran and an accomplished freelance security writer. She has 25 years' experience in communications from working with more than 20 software firms. Jon Friedman is a managing consultant at CyberEdge Group. He has 20 years' experience in industry analysis and marketing from working with more than 40 software, computer, and IT services companies.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-05-8

9 781948 939058