Brought to you by:

CyberGRX

Third-Party Cyber Risk Management

for dummies®

A Wiley Brand

Prevent security threats from third parties

Avoid costly financial and reputational loss

Benefit from automated risk assessment

CyberGRX Special Edition

Fred Kneip, CEO, CyberGRX
Michelle Krasniak

About CyberGRX

CyberGRX standardizes third-party cyber risk management, making it possible to achieve insights, prioritize risks and make smarter decisions across your entire vendor ecosystem. Driven by sophisticated data analytics and automation, real-world attack scenarios, and real-time threat intelligence, CyberGRX provides customers comprehensive and ongoing analysis of their vendor portfolio. Organizations can now effectively manage their cyber risk reputation by proactively utilizing the CyberGRX Exchange to complete and share a single assessment with multiple upstream partners. Learn more at www.cybergrx.com.

Third-Party Cyber Risk Management

CyberGRX Special Edition

by Fred Kneip, CEO, CyberGRX and Michelle Krasniak

for dummies®
A Wiley Brand

Third-Party Cyber Risk Management For Dummies®, CyberGRX Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-88702-7 (pbk); ISBN 978-1-119-88703-4 (ebk)

Publisher's Acknowledgments

Development Editor: Rachael Chilvers
Project Editor: Mohammed Zafar
Acquisitions Editor: Ashley Coffey
Editorial Manager: Rev Mengle
Business Development Representative: Jeremith Coward
Project Coordinator: Melissa Cossell

Foreword

For more than 30 years I've worked as both a cybersecurity professional as well as an advisory board member, lending my expertise in cybersecurity, compliance, and risk management. I'm lucky to have worked with some of the best minds in the business and with teams who are changing the game when it comes to detecting and preventing cyber threats.

One trait of the most successful and resilient infosec teams is being able to make rapid — yet smart — decisions based on data collected. But, as any analyst will tell you, sound business decisions start with clean, relevant, and *actionable* data. Data without insight is just noise, and there's a lot of noise in cyber risk management.

And that's the challenge facing many organizations when it comes to managing third-party cyber risk. Many solutions and tools provide cyber risk data, but rarely does this data enable the advanced analysis that is necessary for true cyber risk management. Teams are used to working within the limitations of these tools; they're used to making do with what they are given.

But what if I told you, that doesn't have to be the case anymore? That there's an approach to third-party cyber risk management that provides the insight into the cyber risk postures of every third party in your ecosystem? This guide flips the script on traditional third-party cyber risk management and discusses how to become part of the future of TPCRM.

I've built my career on forecasting the future of business and creating clear strategies to deliver new and secure operating models for a digital economy. I can say without hesitation that taking a data-driven approach to TPCRM *is* the future of managing cyber risk.

And the future is here.

Edna Conway

Vice President, Global Security, Risk & Compliance, Azure, Microsoft

Introduction

It seems that not a week goes by without a data breach or some other kind of cyber attack topping the headlines.

The targets used to be larger organizations that the bad actors know receive (and store) sensitive customer information such as personal identifiable information (PII) like social security numbers and credit card numbers. These attacks have been quite lucrative in the past.

But there's a new type of cyber threat that has been making the news more and more in the last few years — third-party cyber attacks where the hackers target one organization with the explicit purpose of gaining access to the systems of the companies that the victim organization does business with.

The damage is exponential and what makes this so challenging to protect against is the fact that you may not even know you're vulnerable to these threats. It's easy to assume that every organization takes cybersecurity as seriously as you do and you didn't have a way to learn the truth.

Until now.

So sit back and get ready to learn how even though the traditional ways of doing third-party cyber risk management are no longer enough to keep your organization safe from today's cyber threats, there's a revolutionary new approach that you can't afford to ignore.

About This Book

Third-Party Cyber Risk Management For Dummies, CyberGRX Special Edition, discusses this new world of third-party cyber risk management in five chapters: Understanding Third-Party Cyber Risk Management (Chapter 1), Communicating the Importance of TPCRM (Chapter 2), Tackling the Traditional (and Outdated) Approach to TPCRM (Chapter 3), Evolving TPCRM With a Data-Driven Approach (Chapter 4), and Ten Ways to Make Your TPCRM Program Successful (Chapter 5).

Icons Used in This Book

Throughout the book we use little icons in the margins to draw your attention to particularly useful nuggets of information.

REMEMBER

The information marked by this icon is important enough to be emphasized. In other words, don't forget it!

TIP

Look for this icon when you want a few tricks of the trade to guide you on your way to a successful third-party cyber risk management strategy.

WARNING

Though we don't think it's our place to tell you *not* to do something, we point out instances where you should tread carefully! You'll see this icon if that's the case.

Beyond the Book

If you'd like more information about third-party cyber risk management beyond what this book offers, visit `www.cybergrx.com`.

IN THIS CHAPTER

- Managing cyber risk
- Exploring the need for a risk management strategy
- Outlining the role of TPCRM in various departments

Chapter 1
Understanding Third-Party Cyber Risk Management

Cyber risk.

Those words alone can keep chief information security officers (CISOs) awake at night.

Risk represents the potential for damage when a threat source exploits a vulnerability. In the case of cyber risk, it encompasses all the potential threats that are just waiting for the chance to wreak havoc on an organization's systems and networks. Because, as all cybersecurity professionals know, the fallout from that can be catastrophic.

In this chapter we start at the beginning and talk about what cyber risk is, and we break down the different ways to manage cyber risk. Then we discuss where third parties fit into the cyber risk puzzle and dive into a couple of the most recent cautionary

tales from the world of third-party cyber risk management. And finally, we take you through what this unavoidable risk type means to the different departments in an organization.

Defining Cyber Risk

Cyber risk is the possible exposure to loss or harm stemming from an organization's critical systems, such as information or communications systems. It extends beyond damage and destruction of data or monetary loss, and includes theft of intellectual property, productivity loss, and reputational damage.

Determining the components of cyber risk

Several factors contribute towards an organization's overall risk posture (or status) and each one can be understood and considered in the context of ensuring a complete and effective cyber risk management strategy:

- A **threat** is any entity, circumstance, or event that could potentially do harm or have an adverse impact.
- A **vulnerability** is a weakness that could be exploited by a bad actor; otherwise known as a threat source.
- **Inherent risk** represents the amount of risk that exists in the absence of *controls*, which are safeguards to avoid, detect, mitigate, or minimize cybersecurity risks.
- **Residual risk** is the amount of risk that remains after controls are taken into account.

Now for a bit of a reality check: Despite your best intentions, there's no way to completely eliminate risk. But that's okay!

REMEMBER

In fact, you don't really *want* to remove all risk because it's often necessary for innovation, progress, and organizational success. For example, some risks can lead to positive business outcomes, including exploring emerging markets and growth opportunities, expanding operations into new product areas, and partnering with new vendors.

Exploring the different ways to manage risk

Just because you don't necessarily want to get rid of all risk doesn't mean that it shouldn't be managed. In fact, the best way to keep your organization safe in the face of cyber threats is to have a robust risk management program in place.

That brings us to the different approaches organizations turn to when it comes to managing their risk to an acceptable level.

Governance, risk, and compliance/ workflow tools

Governance, risk, and compliance (GRC) and workflow tools help organize and prioritize risk assessment programs across multiple teams and third parties. These tools allow companies to manage and integrate regulated IT operations in their entirety. Some have specific third-party risk management modules, though they are often limited in their scope and functionality.

Security rating tools

Security ratings attempt to quantify the cyber risk associated with an organization by aggregating various external data sources. Those sources can include news sources, breach aggregators, credit card investigations, internal breach disclosures, chatter on the dark web, and sometimes even social media. While security rating tools can be used on their own, they're only one part of a third-party cyber risk management program.

REMEMBER

While all these vendor risk management methodologies are effective to a degree, risk can't be completely eliminated, so it's important to set proper expectations with your organization's stakeholders.

If you decide to go with a programmatic approach (discussed next) instead of a tool-based approach, GRC tools are typically also instituted to deal with various industry-driven risk and compliance needs.

Third-party risk management programs

A third party is an entity that provides a product or service directly to your customers and/or an entity critical to maintaining your

daily operations and can include partners, consultants, vendors, or suppliers.

Third-party risk management, or TPRM, is the act of identifying and addressing any type of risk (for example, financial, fraud, or cyber) that's associated with third-party entities.

Third-party cyber risk management (TPCRM) is a subset of TPRM and is the act of identifying and addressing cybersecurity-related risks that are associated with your third-party entities. (It also happens to be the main subject of this book!)

TIP

GRC tools are helpful when it comes to managing the workflow of a TPCRM program.

Vendor risk management programs

Vendor risk management (VRM) is the act of identifying and addressing any type of risk that's associated with vendor entities. A vendor is a type of third-party entity that provides a product or service directly to you. All vendors are third parties, but not all third parties are vendors. For example, a contractor or consultant is a third party but not a vendor. VRM solutions are software platforms used for assessing, monitoring, reporting, and remediating vendor risks.

TIP

Think of VRM as the foundational concept of all third-party risk management solutions.

Illustrating the Need for a TPCRM Strategy

The different cyber risk management methodologies discussed in the previous section all serve a purpose, and that's to help protect your organization against cyber threats such as:

- Data breaches
- Theft of data, IP, or equipment containing sensitive data
- Malware (including ransomware)
- Fraud
- Email-based phishing attack

- Denial of service attack
- Malicious insider
- Geopolitical risk

Each of these attack modalities can be catastrophic if not detected and mitigated early on, and security professionals know this. In fact, as you can see in Figure 1-1, most respondents to a recent study conducted by Forrester Consulting stated that these were very concerning.

FIGURE 1-1: All these threats can be the result of bad actors targeting third parties.

But they all have something in common — something that you have less control over.

WARNING

These cyber threats are often the result of bad actors targeting a company's third parties. In other words, oftentimes cyber criminals use these attack methods to gain access to the mission critical systems of the companies the victim organization does business with.

Cyber attacks don't just come at you head on anymore. This is why every enterprise needs to establish a third-party cyber risk management strategy.

WARNING

GRC/workflow tools, security ratings, and general VRM solutions don't focus specifically on third-party cyber risk, so you need to investigate additional solutions to ensure you're protected.

Explaining with Real World Examples

In recent years, cyber criminals have realized how lucrative targeting an organization's third parties can be. They've learned that they can get the most bang for their criminal buck when they focus their efforts on gaining access to the systems of companies who act as third parties to other organizations.

To illustrate this, here's the story of Bob. Bob the Bad Actor knows that a major global retailer will have a top-of-the-line cybersecurity protection system set up. He knows this world-class infosec team is ready and waiting for him and his cunning criminals to try and breach the retailer's cyber borders.

But Bob's team is too lazy to try to infiltrate the retailer's systems directly. It would be difficult and take too much time. That is, if they were able to gain access at all.

Instead, Bob learns that the retailer works with a specific heating, ventilation, and air conditioning (HVAC) company and guesses that this HVAC vendor *doesn't* have a solid cyber risk management strategy in place.

As a result, Bob and his criminal cohorts launch a cyber attack against the HVAC company and easily gain access to their business systems.

Unfortunately, those weakly secured business systems provide backdoor access to the global retailer's own systems.

As a result, Bob and his team end up stealing up to 40 million credit and debit card numbers of the retailer's customers. When the dust settles years later, the retailer is fined $18.5 million, which is a drop in the $200 million bucket the attack cost when it was all said and done.

Does this scenario sound familiar? It should . . . because the Target hack of 2013 goes down in history as one of the biggest breaches to hit a US retailer, and it happened because of the relationship Target had with a third party that didn't have sufficient cybersecurity protections in place.

THE STUFF OF NIGHTMARES . . .

Here are more cautionary tales of security breaches.

SolarWinds

In March of 2020, a hacker group believed to be affiliated with a foreign government gained access to computer systems belonging to multiple third parties. The hackers compromised the infrastructure of SolarWinds, a company that produces a network and applications monitoring platform, and then used that access to distribute updates containing trojans to SolarWinds' users.

At the time, SolarWinds' customer list included 425 of the US Fortune 500, the top ten US telecommunications companies, the top five US accounting firms, all branches of the US Military, the Pentagon, the State Department, as well as hundreds of universities and colleges worldwide. The company has estimated the breach cost at least $18 million in the first three months of 2021 alone, and costs are still adding up as lawsuits are being filed.

Kaseya VSA

During the July 4th holiday weekend in 2021, a state-sponsored hacker group injected ransomware into the networks of Kaseya, an IT management software company, gaining access to the networks of Kaseya's customers. It's reported that the hackers demanded around $45,000 from most of Kaseya's customers, but due to the number of customers affected, the total amount of ransom they demanded was an estimated $70 million.

According to Kaseya, up to 1,500 of their 37,000 customers were affected. However, when you consider that 70 percent of those were managed service providers (MSPs) that had hundreds if not thousands of customers themselves, that number grows exponentially.

Accellion

The Accellion data breach, first discovered in December 2020, was a result of vulnerability in a file transfer system used by many organizations globally.

The Accellion File Transfer Application (FTA), which was specifically designed to move large amounts of data, allowed bad actors to

(continued)

(continued)

access troves of sensitive data from many companies all over the globe. Despite being nearly 20 years old, hundreds of organizations in the finance, government, and insurance sectors use the Accellion FTA product to transfer sensitive files.

The company scrambled to patch the zero-day security vulnerability in FTA when it learned of it in mid-December; however, the zero-day security vulnerability was just one of the anomalies.

The total amount the breach cost Accellion is unknown, but one of its affected customers, Kroger, agreed to pay $5 million to over 3.8 million pharmacy customers whose sensitive information was compromised because of the hack.

WARNING

Cyber criminals have learned that targeting third parties is generally the quickest — and most lucrative — way to launch a cyber attack. Since these attacks are typically high-profile, the media coverage is significant, which means these hacker groups gain notoriety as well as fatter wallets.

Determining Digital Transformation's Role

Digital transformation is the adoption of digital technology into all areas of a business with the end goals being improved efficiency, value, and innovation.

In today's global economy, there's no escaping it. But even though digital transformation is understood to be critical, its rapid adoption, as evidenced by the dramatic growth of cloud providers, Software-as-a-Service (SaaS) companies, and Internet of Things (IoT) devices, is creating significant vulnerabilities for most organizations.

Add to this adoption the practice of Shadow IT — installing software without the knowledge or approval of the company's IT department — and digital transformation has the potential to be extremely worrisome.

A recent Ponemon Institute study found that digital transformation increased a company's reliance on third parties and showed that the average enterprise works with over 5,800 third parties, with 200 of said third parties having access to the company's systems on any given day.

Fifty-eight percent of respondents reported not having a proper (or any) third-party cyber risk management program in place to ensure that the vendors they're doing business with are following good cybersecurity practices. This lack of visibility leaves every interconnected organization vulnerable.

And the numbers are showing that, as 82 percent of respondents in the Ponemon study stated, their organization experienced at least one data breach because of digital transformation and 55 percent could say with certainty that at least one of the breaches was caused by a third party. (See Figure 1-2.)

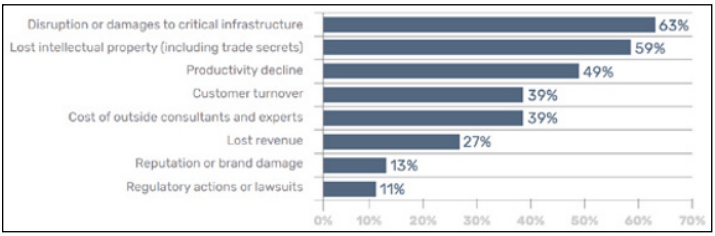

FIGURE 1-2: There were many consequences of these data breaches.

Outlining what TPCRM Looks Like for Different Departments

Third-party cyber risk management doesn't — and shouldn't — happen in a vacuum. In fact, several departments are stakeholders when it comes to working with third parties, even if they may not be working with them directly.

REMEMBER

For this book, we've listed three of the most common stakeholder departments and their role in the process. Depending on your organizational size and structure, you may have additional — or fewer — departments involved in the third-party cyber risk management lifecycle and there may be differing responsibilities.

Security

The security team at an organization is responsible for protecting people, assets, infrastructure, and technology. Security teams must develop and maintain the security program of an organization in a balanced way that considers the current and evolving security landscape along with the organization's business goals, needs, and resources.

Some key responsibilities include:

- Establishing and executing security and governance practices to contribute to business goals and overall success.
- Educating and training employees on current and future security challenges.
- Supporting business operations with the right tools and capabilities that meet security and compliance needs while using company resources efficiently.
- Monitoring, preventing, detecting, and responding to security threats within the organization as well as recovering from incidents, ensuring business continuity.

When different departments introduce new third parties into an organization, it's the security team who's responsible for ensuring that this new vendor's cybersecurity practices are adequate and that there are no areas of concern. If there *are* concerns, the security team determines if the residual risk is acceptable. (See the section "Determining the components of cyber risk" earlier in the chapter).

Risk management

The risk management team is tasked with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's productivity and profitability. They are the first line of defense when it comes to a company's cyber risk reputation management.

The team owns the implementation of operational management and mitigation processes to avoid losses stemming from inadequate or failed procedures, systems, or policies. This often includes business continuity and disaster recovery planning, programs focused on governing regulatory compliance data, as well

as providing input on IT or information security processes to the security team.

Key responsibilities include:

- Integrating risk management priorities into the company's overall strategic plan, typically through development of risk maps and action plans that mitigate the primary threats.
- Developing and disseminating risk analysis reports monitoring the progress of mitigation efforts to executives and board members.
- Creating and implementing strategies to protect against and manage risk related to the use, storage, and transmission of data and information systems.
- Conducting due diligence and risk assurance during business deals, mergers, and acquisitions.

Risk management professionals access relevant third-party data to better view and prioritize cyber threats and risks. So, when there's an effective, streamlined third-party cyber risk management program in place, this team can quickly and efficiently report on the company's overall risk posture to stakeholders including the C-suite and board of directors. (For more information on communicating with stakeholders, see Chapter 2.)

Procurement

The Procurement team typically focuses on the areas of purchasing, strategic sourcing, contract management, and risk management. Their goals include ensuring cost-effective and timely purchasing decisions, developing and managing supplier relationships, and encouraging innovation and diversification of the supply chain in order to help the business meet its needs.

Key responsibilities include:

- Reducing cost through discounts and contract negotiations.
- Aligning purchasing decisions with the compliance and regulatory needs of the business.
- Managing the risks of purchasing decisions that include reputational, financial, liability, and availability.

When it comes to TPCRM, the procurement team knows the importance of diversifying the organization's third-party network to ensure the security of supply chain.

They're the folks behind the scenes making sure that if one of the organization's third parties *does* have a cyber incident and is unable to provide goods and services, that it doesn't negatively affect the enterprise's ability to still provide goods and services to *their* customers because a different vendor can be utilized in its place.

REMEMBER

While it's a good idea to diversify your supply chain, doing so increases the attack surface area the security and risk teams have to manage.

IN THIS CHAPTER

- Securing leadership's support
- Ensuring the board is on board
- Tying it all together for other stakeholders

Chapter 2
Communicating the Importance of TPCRM

When it comes to moving a business forward, the time inevitably comes when you need to implement new tools and processes to get things accomplished, and sometimes it takes a little convincing to get others on board with the direction you want to move in.

In this chapter we explain how to have important conversations about the need for a comprehensive third-party cyber risk management strategy. From the CEO and CISO to the board of directors and other stakeholder departments, we discuss how to communicate the benefits that come with a robust solution, and the risks associated with maintaining the status quo.

Getting Buy-In from Leadership

Globally dispersed, highly networked, and digitized businesses face new cybersecurity and resiliency risks that many organizations are just starting to address.

When it comes to cybersecurity, an enterprise's security is significantly impacted by the security of their third-party vendors, which oftentimes handle mission-critical and sensitive data. As a result, organizations are establishing third-party cyber risk management (TPCRM) programs to better identify, assess, mitigate, and oversee the risks created by third parties in their digital ecosystem.

Each organization within an enterprise plays an important role in the success of a TPCRM program. In the light of competing priorities, it's important to collaborate and communicate with the stakeholders how having an effective cyber risk management program in place can enable them — and the company — to be successful.


TIP

Start with the why. It's the subject of a popular book on leadership by Simon Sinek, but the concept applies to many areas in life. When communicating with different stakeholders in the company, start with *why* having a robust cross-functional third-party cyber risk management program in place will not only keep the organization safe from cyber threats, but can also enable everyone to be successful in their job function.

Teaming up with the CEO

The CEO (oftentimes in conjunction with a board of directors), is concerned with the business strategy, growing revenue, and improving operations. Because of this, it's important to communicate that having a TPCRM program in place will help the company meet its business goals.

As enterprises look to increase global competitiveness and agility, they're rapidly adding new technology and partners into the fold. Digital transformation and the increased need to outsource means more inherent risk. It's vital to have a strategy in place to quickly and accurately perform due diligence on these vendors and tools to assess the risk.

Investing in a TPCRM solution that helps identify and manage risk at scale enables organizations to more quickly deploy cloud-based tools, analytics platforms, and other tools used to continuously transform and propel the business forward — without sacrificing security.

REMEMBER

With 63 percent of breaches being due to a third party being compromised, there's a need to quickly, easily, and accurately assess the risk of potential vendors, to protect both the businesses' bottom line and reputation.

Partnering with the CISO

Chief information security officers (CISO) work hard to keep data and applications secure. Security teams must develop and maintain the security program of an organization in a balanced way that takes into account the current and evolving security landscape along with the organization's business goals, needs, and resources.

But security is about more than just defense. It's now the lynchpin to an enterprise's plans for transforming operations and growing revenue. When a breach happens, a company's reputation is severely damaged, and as any executive can tell you, reputation is directly tied to a company's bottom line. It can take years for an organization's reputation to rebound — if it does at all.

The landscape of TPCRM is evolving, driven by increased cyber threats and attacks aimed specifically at third-party providers and supply chain vendors. For organizations to effectively protect against these threats, they must focus on the cyber-centric data in order to make quick, well-informed decisions.

TIP

Companies need to ensure trust with customers and partners, and one way to do that is to demonstrate the ability to keep data secure. By identifying and managing emerging threats and risk inherited from third parties quickly and easily, they can meet the expectations of existing customers and procure new business.

REMEMBER

It's essential to scale the due diligence and risk identification process to meet the needs of the business. As companies grow, they're bringing on more third parties and technology, so having a third-party cyber risk management solution in place can provide an objective source of information to help the organization make critical decisions quickly and with confidence.

Security teams can lead the charge in this area with better education and collaboration tools to show how a new approach is needed that goes beyond compliance to true cyber risk management.

Speaking with the board

An enterprise's board of directors is interested in projects that help modernize and transform the business to improve performance and increase revenue.

Oftentimes, however, the board is made up of people who have built their careers in disciplines such sales, finance, or business. They bring to the table a lot of expertise in their respective areas, but it's not common to find a cybersecurity executive sitting on a board. In fact, most boards assume their IT and security teams have cybersecurity covered. But with the number of third-party cyber incidents rising annually, boards are starting to pay closer attention.

For example, investors in SolarWinds recently filed a lawsuit against the company's board because of the 2020 breach. (For more information on the breach, refer to Chapter 1.) The investors claim that the board of directors knew about the cybersecurity flaws ahead of time yet failed to heed the warnings and mitigate the risks.

The lawsuit alleges that there weren't any procedures in place to monitor cybersecurity risks, such as requiring the company's management to report on those risks on a regular basis. In addition to monetary damages, the investors are seeking to reform the company's policies in this area.

WARNING

This is believed to be the first lawsuit of its kind, but also one that opens the doors to others in the future.

Incidents like this could possibly be avoided if an organization has in place a comprehensive third-party cyber risk management strategy that identifies the third-party ecosystem, prioritizes it, assesses the risk present, and then mitigates risks that are unacceptable.

The right solution doesn't just check a bunch of boxes for the sake of compliance; it provides a thoughtful approach that includes a portfolio-wide view to spot third-party weaknesses. Organizations should consider how to deepen third-party assessment analysis, standardize processes, and improve the quality of tools used.

REMEMBER

Implementing these changes helps organizations improve the quality of their third-party risk management programs, strengthening their ability to prevent and respond to threats. The data collected can be used when it comes time to report to the board, thereby giving them the visibility necessary to make smarter decisions about their cybersecurity health.

Working with Other Stakeholders

As we've mentioned before, having a comprehensive, robust, and effective TPCRM program in place shouldn't happen in a vacuum. In fact, it can't.

Arguably every department in every company utilizes outside vendors for goods and services at some point. Maintenance needs cleaning supplies. Finance works with audit teams and maybe a courier service. The executive team may get catered lunches from time to time. Even having a corporate credit card means you're working with a third party.

REMEMBER

Third-party cyber risk management isn't just the CISO's or IT department's challenge to overcome in a silo.

In Chapter 1 we briefly talked about how TPCRM fits into the worlds of the security, risk management, and procurement teams. Here we give you some ideas on how to successfully communicate the importance of implementing — and then following — a third-party cyber risk management strategy for those departments who aren't always in the thick of things.

Legal department

The legal department is a stakeholder department and should be considered *before* their input is needed due to a cyber incident!

They're responsible for finalizing contracts with partners and vendors, reducing risk, and meeting compliance requirements.

So how do TPCRM tools make their lives a little easier? The tools provide organizations with a faster, independent, and defensible method for assessing risk and performing due diligence. The detailed, validated reports are granular, accurate, and dynamic, so they keep pace with changes made by vendors and partners, thereby offering the most current view of risk.

REMEMBER

According to Gartner, 80 percent of legal and compliance leaders say third-party risks were discovered *after* initial onboarding and due diligence. That's too late in the process. It not only increases the risk to the organization, but it means delays in realizing the business value from those relationships. A third-party cyber risk management solution can prevent last-minute surprises.

Privacy

While every organization may not have a separate department dedicated solely to privacy (except as required by regulatory bodies), this may change in the future as more and more attention is being paid to data privacy and what it means for both companies and consumers. Those individuals who oversee privacy concerns should be considered stakeholders in TPCRM matters.

This team, led by the chief privacy officer (CPO), is responsible for developing and implementing policies designed to protect employee and customer data not only from unauthorized access, but also to ensure that the data is being used appropriately.

Since businesses increasingly rely on technology from third-party vendors (such as cloud platforms and SaaS applications) to store and analyze data, they need a process to quickly and thoroughly complete due diligence.

A third-party cyber risk management solution offers a way to scale efforts and provide continuous threat monitoring that keeps pace in a rapidly changing areas of the business. Being able to look at privacy controls and security controls through the same lens gives a clearer picture of your third-parties' privacy programs.

As businesses become more data centric, data security becomes mission critical. Consumer trust in businesses to maintain the privacy and security of their data is already low, and any breaches or data leaks will result in further deterioration of those relationships. Having a TPCRM strategy in place helps uncover how well third parties identify, govern, control, communicate, and protect privacy data.

IN THIS CHAPTER

- (Re)Assessing assessments
- Dealing with noisy data
- Looking toward the future of TPCRM

Chapter 3
Tackling the Traditional (and Outdated) Approach to TPCRM

The traditional approach to third-party cyber risk management is wrought with redundant and inefficient processes. It costs precious time and resources that already-strapped security teams don't have enough of. As a result, risks are inadvertently overlooked, and companies remain vulnerable.

In this chapter we outline the current approach to TPCRM and take you through everything that's wrong with it. From assessment chasing and static spreadsheets to vendor backlogs and data that's nothing but noise — we cover it all.

But we also introduce you to the light at the end of the tunnel: the future of third-party cyber risk management.

Assessing Third Parties

The National Institute of Standards and Technology (NIST) defines risk assessments as tools used to "identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems."

The primary purpose of a cyber risk assessment is to collect critical cybersecurity data to allow for timely responses to identified risk. When an organization has visibility into the cybersecurity health of the third parties they do business with, they're able to make well-informed decisions to keep the business safe.

But assessments aren't without fault (or headaches). It's safe to say that people don't really *like* to fill out assessments time and time again, but they've accepted it as a necessarily evil. In the following sections we break down some of the most common frustrations and limitations with cybersecurity assessments.

Chasing assessments

Assessment chasing is when you've requested a cybersecurity assessment from a current or potential third party and you find yourself needing to constantly follow to get it completed.

Sometimes organizations haven't kept pace with business demands or budget constraints have lead to small IT teams. These teams are tasked with filling out these assessments in addition to their day-to-day responsibilities of keeping the company's systems and data safe from cyber threats.

WARNING

When IT teams are filling out assessment after assessment, that means time is being taken away from actually managing their company's risk; something that leaves them more vulnerable.

Security assessments are typically also very long, comprehensive, and sometimes require evidence to prove what's being claimed. A Ponemon Institute study found that third parties spend an average of 15,000 hours *a year* filling out assessments for their customers and prospects. It's no wonder that it's sometimes hard to get the assessments completed in a timely manner!

But third parties aren't the only ones experiencing delays and frustrations with the assessment process. For the first parties (in other words, the organizations requesting the assessments), these delays mean additional resources needing to be expended to ensure the assessments get completed. And more troubling, when assessments aren't completed in a timely manner, the first party is left vulnerable to unknown risks for however long it takes to receive the completed assessment. Furthermore, this risk trickles down and eventually affects the departments who are unable to continue with business relationships and/or services until they get the greenlight from the security/risk management teams.

The bottom line is that the assessment process is full of frustrations and headaches on both sides of the table.

Filling in static spreadsheets

Great! The third party took the time to fill out the assessment, hopefully with little to no chasing required! Now what?

Well, if you're like many organizations, the information in the assessments gets put into a static spreadsheet. A spreadsheet containing cyber risk data that theoretically could be changing as you're reading it. In other words, traditional risk assessments are snapshots, or point-in-time captures of the cybersecurity health and practices of a single company. They're not a complete picture of the risk landscape your organization is facing.

This is a big problem for both of the parties involved. It's troublesome for the requesting company because you can never be sure if it's the current status of the third-party's risk posture. Maybe they had a data breach a month after you got the assessment back, which would completely change the overall picture of that company's cyber health. Or maybe they've made some major strides in strengthening their cybersecurity practices, and those aren't fairly reflected in this static document.

WARNING

Not having the most up-to-date data for all third parties in your ecosystem leaves you vulnerable to risk you may not even be aware existed.

The reality is, because assessments are long and tedious to complete, many companies don't request them from third parties on a regular basis, so it may be a considerable amount of time since an

updated assessment was completed. It's almost a guarantee that a company's cybersecurity health has changed in some way over the course of a year or more. After all, just like your organization, the third party is adding on vendors of their own, which introduces a concept called *nth party risk.*

REMEMBER

Nth party risk is the risk present due to a company's third parties having their own third parties and so on. The idea is that the risk grows exponentially for all organizations.

Collecting data and not managing risk

We mentioned earlier in the chapter that when it comes to receiving security assessments from third parties, a lot of resources go into "assessing the assessment." In other words, security teams put so much time and energy into collecting and storing the data, that it leaves little time to analyze, manage, and reduce the risks that may be present.

The fact of the matter is, you can have all the data in the world at your fingertips, but if it's not actionable or bring with it insights that you can then use to reduce your cyber risk, then that data is just noise.

Even when the data is collected and analyzed, how complete of a picture does it paint of your organization's risk? Not a very good one unless you're able to look at the assessment data of all your third parties together, allowing you to do benchmarking, glean insights, observe trends, and prioritize your risk mitigation efforts.

REMEMBER

Answering questionnaires and filling in spreadsheets is a tool in the third-party cyber risk management toolbox. It's just not true cyber risk management.

Lacking scalability

We've previously mentioned that a Ponemon study found that the average organization works with over 5,800 third parties. That's *a lot* of security assessments needing to be filled out and data analyzed! The way it's being done today — the assessment chasing and maintaining of static spreadsheets — is not scalable and many organizations can't keep up with the process.

REMEMBER

Many companies invest significant time and resources in the assessment collection process and don't see a return on investment (ROI) that brings a level of confidence needed to truly believe their risk posture is improved. It's often said in cybersecurity that compliance doesn't equal security. In a similar way, due diligence doesn't equal risk management.

TIP

An important hallmark of a good TPCRM program is that it scales with your business.

Tackling backlogs and vendor growth

As if having 5,800 third parties in an average vendor ecosystem wasn't enough, that number is expected to grow by 15 percent year over year. That means, within three years, the average third-party ecosystem of an organization will be over 8,800 vendors!

This rapid growth causes backlog issues, and it's showing. A Forrester study found that, on average, approximately 24 percent of an organization's new third parties and 40 percent of current third parties remain unassessed. And, even when performing these assessments, the organizations only skim the surface of defining the level of risk, leaving out critical components of accurate risk evaluation.

The current method of performing third-party cyber risk management isn't allowing security and risk professionals to accurately and sufficiently manage risk because teams can't keep up. It's become about checking a compliance box, which may keep auditors and regulators at bay, but not bad actors.

Dealing with Data That Isn't Actionable

Once security assessments are received, the analysis starts.

. . . or does it?

That depends. Is the data you've collected actionable? Can you clearly see patterns in how hackers and exploits work in varying environments or benchmark across industries?

Chances are, if you're utilizing a customizable assessment, you won't get this level of insight into your vendor ecosystem. How can you glean insights and make quick, informed decisions if the data you have isn't standardized, consistent, and comparable across your third-party portfolio?

A standardized risk assessment process that collects data in a structured format enables both third parties and enterprises to perform analytics on that data and derive insights. It also reduces the redundancies and inefficiencies that bespoke assessments place on third parties, creating more time for you to focus on strategic risk management.

REMEMBER

Data without insight is just noise.

When you're able to easily see patterns across your entire portfolio of third parties, you can make quick decisions about what risk to mitigate first; which low hanging fruit to pluck, if you will. This way your team can be most effective with the least amount of effort.

Settling for Silos

In Chapter 2 we discussed what third-party cyber risk management (TPCRM) means for stakeholder departments throughout the company. That discussion is applicable in this chapter about the old and ineffective way to managing risk, too. Because when there are competing priorities and decisions must be made, oftentimes people go with the option that serves their department's needs the best. This can have far-reaching negative consequences across the board.

But there's also a more theoretical siloing that contributes to the cumbersome, outdated approach to TPCRM. And that's the lack of cyber risk data sharing that happens among all organizations.

It all comes back to those individual, bespoke assessments this chapter opened with. The process is largely the same: Company A requests a security assessment from Company B. Company B fulfills the request for Company A. Company A stores the assessment data in static spreadsheets until it's time to review and make decisions about the business relationship.

This is done time and time again with all this rich data being stored in the disparate systems of innumerable companies around the world, accessible only by that company's security team.

This is cybersecurity siloing on a grand scale. Siloing that has contributed to vulnerabilities — both known and unknown — that are just waiting to be exploited by bad actors.

Stepping into the Future of TPCRM

It's time for a new approach to third-party cyber risk management. An approach that breaks down those silos to make rich and, more importantly, *actionable* cyber risk data available to companies around the world.

Enter the *risk exchange* and the foundation of a scalable, cost-effective way to manage third-party cyber risk.

In the next chapter of this book, we introduce you to a revolutionary new approach to third-party cyber risk management that gives you instantaneous and unprecedented visibility into your entire vendor ecosystem, enabling you to make well-informed decisions in real-time.

With the help of machine learning, you'll be able to see not only the inherent and predicted risk posture of each vendor, but also monitor and assess them through the lens that matters most to you. You'll have more insight into your third-party cyber risk environment than ever before.

IN THIS CHAPTER

- Starting at the beginning with the exchange model
- Realizing the importance of standardized data
- Changing the game with Predictive Intelligence

Chapter 4
Evolving TPCRM With a Data-Driven Approach

Up until this point we've talked about how the current way to perform third-party cyber risk management is, at best, clunky and inefficient and, at worst, ineffective.

Luckily all that is changing with a new, data-driven approach to TPCRM. In this chapter we look at the foundation of this approach — the *exchange model*. Then we discuss a few key components of this revolutionary new approach. Finally, we introduce the technology that's changing the game entirely.

Utilizing an Exchange Model

In the previous chapters, we discussed the types of collaboration that are important when it comes to effective third-party cyber risk management, including:

- Inter-departmental collaboration within an organization
- Collaboration between first parties (the assessor) and third parties (those being assessed)

» The community-level collaboration that results from the sharing of cyber risk assessments of companies around the world using a shared platform

It's this last type that we'll get into more detail here.

Benefiting from the one-to-many concept

The one-to-many approach to TPCRM enables speed and lowers the cost for all market participants.

For example, when you apply for a new credit card, does someone from the credit card company show up at your door to review your financial history? Of course not! Instead, the company uses credit reporting services like Experian or Equifax to perform the work on an ongoing basis. By utilizing the data, the reporting agencies already have on consumers, credit card companies save time and money when it comes to making decisions on your creditworthiness.


REMEMBER

An exchange works the same way for third-party cyber risk. When third parties fill out risk assessments, that dynamic and standardized data is then made available for other exchange participants to utilize to make their own well-informed decisions about the cyber risk they're exposed to. (See Figure 4-1.)

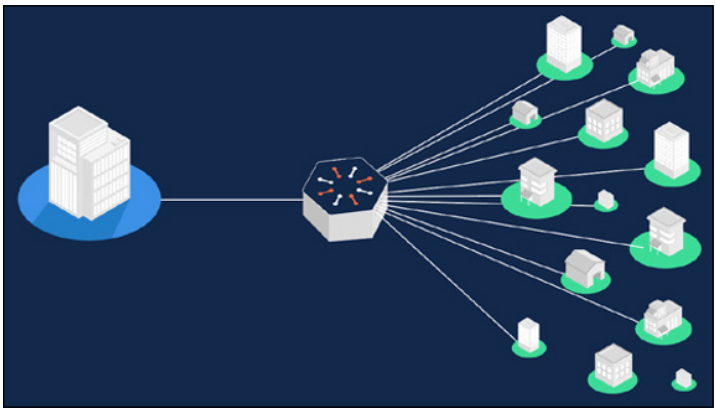

FIGURE 4-1: The one-to-many structure of the exchange model.

TIP

There are three main factors that drive the need to have a more advanced third-party cyber risk strategy in place, and all benefit from leveraging a risk exchange to achieve the scale necessary to succeed:

- More regulatory scrutiny
- Increase in the number of third parties used by enterprises
- More frequent cyber events that involve a third party

Realizing the advantages of standardized exchange data

In Chapter 3 we discussed the importance of the cybersecurity risk data that's collected being *actionable*. In other words, does it provide the insights that enable you and your team to make quick, well-informed decisions in order to protect your company? Or is it just a collection of data that's mostly just being stored somewhere for reference?

Leveraging the data contained within the exchange allows anonymized benchmarking across various groups such as industry or company size that can indicate how a company's security posture stands in relation to its peers. Furthermore, advanced analytics allows for risk analysis across an ecosystem of third parties by integrating risk intelligence data, attack scenarios, assessment responses, and first-to-third-party relationship information.

WARNING

Not all risk exchanges are created equal. The data must be *standardized* to allow for the benchmarking and advanced analytics that bring the ecosystem visibility, and cost and time savings. Standardization on the input leads to better customization on the output.

Another benefit of utilizing an exchange with standardized data is the ability to see your entire vendor ecosystem in one convenient location. You get 360-degree correlated data and rich, diverse analytics to support real-time decision-making, giving you more insight into your third-party cyber risk environment than ever before. We dive deeper into this idea in the next section.

Gaining Complete Vendor Ecosystem Visibility

"You can't see the forest for the trees" is the theme when it comes to the outdated, traditional approach to TPCRM. In other words, when you're looking at bespoke risk assessments one at a time, you're unable to do the necessary analysis to ensure that your organization is sufficiently managing its risk.

Additional reasons your TPRM program should include complete vendor ecosystem visibility are:

- **Benchmarking capabilities.** Being able to see your entire vendor ecosystem through one pane of glass allows you to perform vendor benchmarking across a variety of factors like company size, industry, ecosystem, and similar vendors in the exchange. This can give you insight into the overall cyber health of not only each individual vendor, but also your vendor ecosystem as a whole, allowing you to make smarter decisions.
- **Near real-time threat awareness.** When you're able to view all your third parties at a portfolio level, you can better see where the opportunity for a cyber incident involving one (or more) of them exists. By contrast, bespoke assessments only give you point-in-time glances at the security postures of an individual third party, leaving the rest of the ecosystem unmonitored.
- **The ability to make risk-mitigating decisions quicker.** When you have risk intelligence (an integrated look into your risk posture) at both the individual third-party level and at the ecosystem level, you can pick and choose how to analyze and report on the data. This enables you to view your risk through the lens that makes the most sense to your organization.

Incorporating MITRE ATT&CK

Deriving insights from a cybersecurity assessment requires a framework based on real-world threats. Third parties can be found in virtually all industries and are used by their customers

in distinct ways. This also means they're subject to varied and unique threats.

When assessing a company's inherent risk or prioritizing control gaps for remediation, a TPCRM solution should contextualize each third party with the applicable threats for their industry along with how customers actually engage with them. Enter the MITRE ATT&CK® framework.

MITRE's framework provides the concepts and definitions necessary to ensure TPCRM strategies are "future proof" and facilitate the integration of a tool with threat feeds and other data sources.

Explaining MITRE

MITRE ATT&CK, which stands for *MITRE Adversarial Tactics, Techniques, and Common Knowledge*, is a knowledge base of tactics and techniques used by bad actors in cyber incidents. It's based on real-world observations and the "reverse engineering" of past attacks, reflecting the various phases of an adversary's attack lifecycle and the platforms they're known to target. The framework is used as a foundation for the development of specific threat models and methodologies in various industries, including the government and private sector.

What this means for you is that there is a publicly accessible database for organizations — including cybersecurity companies — to use in order to create products and services that improve the cybersecurity risk postures of their customers, based on real-world attacks and threats.

Why is this an important feature of a third-party cyber risk management solution? It's because bad actors are constantly honing their craft. They're on a non-stop quest to outsmart and outwit even the most advanced and expensive cybersecurity measures. The only way to stop them is to beat them at their own game, and that translates into taking their past attacks and analyzing them in order to develop better offensive and defensive measures.

REMEMBER

Effective risk management that integrates the MITRE ATT&CK framework into a solution is another way to collaborate with the cybersecurity community.

Using threat profiles

Threat profiles are use cases that bring together the type of bad actor, their target(s), and the attack lifecycle (otherwise known as a *killchain*) as a series of MITRE techniques used to achieve the compromise.

A threat profile is created by examining tactics and techniques from hundreds of use cases, including past attacks, in order to identify the primary controls needed to detect, prevent, and mitigate threats. This data can then be used in ongoing threat monitoring and remediation efforts.


TIP

When threat profiles are incorporated into a TPCRM solution, organizations can take advantage of the visibility into how a third party aligns against each identified control. If any controls are missing or absent, the company can follow up with the third party in question to request remediation.

Understanding security ratings

Security ratings attempt to quantify the cyber risk associated with an organization by aggregating various external data sources. These are publicly available and can include news sources, breach aggregators, credit card investigations, internal breach disclosures, chatter on the dark web, and sometimes even social media.


REMEMBER

Security ratings alone aren't a sufficient means of managing third-party cyber risk; however, they're very useful when used as part of a holistic TPCRM approach that includes other methodologies like risk assessments and security audits.

The analysis done to determine security ratings is very comprehensive, as you can see in the list below. The following security domains are commonly taken into consideration:

- **Software patching.** This includes information about application servers, OpenSSL, CMS, web servers, email servers, and DNS servers.
- **Application security.** CMS admin authentication, HTTP security headers, unencrypted sensitive communications, and links to malicious sites are the security criteria looked at.

- **Web encryption.** This includes certificate expiration, certificate valid date, hash algorithm, key length, encryption protocols, certificate subject.
- **System reputation.** The data looked at here includes information about C2 servers, botnet hosts, hostile-hosts: hacking, hostile-hosts: scanning, phishing sites, other blacklisted hosts, spamming hosts.
- **Breach events.** This one is self-explanatory! This is information disclosed about recent and historical breaches.
- **System hosting.** Includes data about shared IP hosting, hosting fragmentation, hosting countries, hosting providers, hosting domain surface, and hostname surface.
- **Email security.** This category includes email authentication (SPF/DKIM), and email encryption.
- **DNS security.** The data analyzed includes information on domain hijacking protection and DNS hosting.
- **Network filtering.** Included in this category is unsafe network services and IoT devices.

But what happens when you don't have the third-party's own assessment data to compare with? The security domains we've just discussed can still provide value, but they need the third-party data to be applied against. Enter *predictive risk intelligence*.

Exploring Predictive Analytics

In Chapter 3 we talked about one of the frustrating realities of security assessments — assessment chasing. In other words, having to chase down the person or persons at the third party who's responsible for completing the assessment. And as a third party, having to complete hundreds, sometimes thousands, of assessments that are similar but not quite the same.

We also talked about how assessments are a static, point-in-time snapshot of the cybersecurity posture of a third party and how the data in the assessment could be outdated and you wouldn't even realize it (until it was too late!).

What if there was a way to get the benefits of a security assessment without having to struggle with getting it completed by the third party in question?

Or if you're the individual tasked with filling out hundreds of these assessments a year, what if there was a way to provide immediate risk insights results to customers, allowing for prioritization of requests for self-attested assessments?

Now there is!

Incorporating predictive risk intelligence

To have an effective third-party cyber risk management strategy, it's important that the tools and solutions you utilize be dynamic and comprehensive.

REMEMBER

Cyber threats are constantly evolving and your TPCRM approach should, too.

This is where predictive risk intelligence comes into play.

Predictive risk intelligence applies the power of machine learning to an exchange database containing assessment data from tens of thousands of companies to provide unique insights across third-party ecosystems. This means you can make quick, well-informed decisions about your organization's cyber risk with a high degree of confidence.

From inherent and residual risk views, to mapping against common and customized frameworks, to providing control gap analysis using threat profiles and real-life cyber-attack analytics, predictive risk intelligence allows you to monitor and analyze your third-party risk through whatever lens you choose.

Uncovering Predictive Risk Profiles

Predictive Risk Profiles forecast how a given third party will answer assessment questions based on factors like firmographics, threat intelligence, outside-in data, and similar completed assessments on the exchange with up to an 85 percent accuracy rate.

TIP

When a risk exchange is based on standardized data from thousands of companies, a Predictive Risk Profile can be created for every company. Each company can then view and share their risk profile as they see fit, enabling transparency and collaboration to address control gaps and risk remediation strategies.

Benefits for those companies seeking to manage their third-party risk include:

- **Instant insights.** Instantly view comprehensive and actionable Predictive Risk Profiles for each third party.
- **Stop the chase!** Instead of chasing assessments, you can spend valuable time and resources analyzing data and remediating risks discovered.
- **Prioritization.** Rank your critical and high risks by using Predictive Risk Profiles, MITRE ATT&CK scenario analytics and threat profiles based on real-world cyber events.
- **Manage your reputation**. Utilize your own Predictive Risk Profile to better manage your cyber risk reputation as a third party to your own customers.

For third parties that often find themselves drowning in assessment requests, Predictive Risk Profiles offer the following benefits:

- **Bridge the gap.** Provide immediate risk insights results to customers, allowing for prioritization of requests for self-attested assessments.
- **Save resources.** Share your assessment with other requesters to save time and resources in responding to multiple requests.
- **Become informed.** Use built-in tools to better understand control gaps and threat profiles to compare vulnerabilities to exploits used in real-life cyber attacks.

PREDICTIVE RISK PROFILES USE CASE

Before Dave Stapleton joined CyberGRX as their CISO, their security team spent extensive time on manual, tedious work within spreadsheets and various types of documents related to third-party risk assessments.

His challenge isn't unique in the role of the CISO where, instead of allocating resources toward initiatives and activities that drive the business forward, security teams spend considerable time chasing assessments.

Predictive Risk Profiles empower Dave to harness the power of machine learning to view instant, predictive risk assessment results for every third party in the organization's portfolio. Now, he has the insights to prioritize the critical areas of risk in his organization's vendor ecosystem without the overhead typically required to collect this data.

These instant insights set him and his team up to initiate more informed risk-based discussions with vendors and business partners, ultimately cutting down on the time needed for third parties to respond to assessment requests, allowing for them to instead create more effective and efficient relationships.

The Predictive Risk Profile provides analysis through machine learning that predicts how a given vendor will answer each assessment question based on firmographics, outside-in data, and similar completed assessments on the Exchange.

These instant insights allow security teams to view inherent and residual risk to map against common and custom frameworks and provide control gap analysis using threat profiles and real-life cyber-attack analytics.

By leveraging Predictive Risk Profiles, Dave and his team can more efficiently analyze their third-party risk through the lens that matters most to them, based on their custom framework.

The ROI/value created:

- **Time reduction.** The Exchange has significantly reduced the time it takes Dave and his team to conduct third-party cyber risk

assessments, enabling them to effectively manage 85 percent more of their ecosystem. Plus, other teams within his organization can access third-party tools much quicker now that the security team can lean on Predictive Risk Profiles to speed up the procurement process operationally.

Although Dave and his team still intend to order assessments from all vendors in their portfolio, they'll be able to provide preliminary approvals much quicker.

- **Resource allocation.** The Exchange, paired with the new functionalities of Predictive Risk Profiles, allows him and his team to spend less time hunting down assessments. Now, he can reallocate his time to evaluate and remediate known security risks, engage in market-facing activities — such as speaking at events and panels — create leadership content to advance the security community at large, and make informed decisions that drive the business forward.

  Lastly, Dave can broaden the scope of his current responsibilities. People often have questions about their organization's security posture, for example. Dave can hop on a call and build confidence around his organization's security posture, providing a perspective only he can, which ultimately builds stronger relationships with potential customers.

- **Continuous insight.** Much of the manual work spent gathering assessments doesn't require any cybersecurity education or experience, yet cybersecurity professionals are usually those tasked with the job.

  In an industry that struggles to find qualified professionals yet has no shortage of security-specific tasks, this use of time is not providing the highest value to organizations. The instant and comprehensive insights provided in the Exchange can allow Dave and his team to exercise their skillset, analyze risk, and drive the business forward without adding additional overhead.

IN THIS CHAPTER

- Exploring the importance of scalability and visibility
- Tying it all together with automation and education

Chapter 5
Ten Ways to Make Your TPCRM Program Successful

Throughout this book we take you through the challenges facing security and risk practitioners when it comes to protecting their organization from third-party cyber risk. In this chapter we put it all together for you and give you ten ways to make your third-party cyber risk management (TPCRM) strategy successful now and in the future. Let's get started!

Scalability

The goal of every business is to grow revenue, but to do that, you have to grow your team and the number of third parties and vendors you do business with. Unfortunately, both increase the number of attack vectors that bad actors can exploit.

In order to ensure your company's cybersecurity stays . . . well . . . secure, your third-party cyber risk management strategy needs to be able to grow with you. That's why using static spreadsheets to track and perform analysis isn't a long-term viable solution. You need to utilize a risk management tool that can grow with you to ensure uninterrupted protection and that is beneficial to all stakeholders across the organization.

Complete Visibility

Notice we say *complete* visibility. It's no longer sufficient to just have a glimpse into the cyber risk posture of your third parties on an individual company level. It's imperative that you're able to see the health of your entire vendor ecosystem to make rapid, well-informed decisions.

When you have complete third-party portfolio visibility you can see not only the inherent and predicted risk posture of each vendor, but also monitor and assess them through the lens that matters most to you.

Data-driven Approach

Data tells a story unlike anything else. As humans, we don't always pick up on things like trends or discrepancies. But when viewed through the lens of the data, you're able to identify trends and create benchmarks that facilitate smarter decision making.

The key is that it must be standardized data (accessed through risk assessment exchanges) as that's where you'll get the actionable insights needed to proactively identify and mitigate third-party cyber risk.

Continuous Monitoring

Bad actors don't take vacations or celebrate holidays. In fact, they know many companies (and security teams) are working with skeleton crews, so cyber threats are more likely to go unnoticed during these slow times. Because of this, your TPCRM solution

should provide continuous monitoring capabilities to ensure your vendor ecosystem stays secure, regardless of the date.

Continuous monitoring is also important because relationships with third parties change and evolve over time, including the expansion or decrease of services, changes to location or facilities, and so on. Continual monitoring is vital for the health of the relationship and the safekeeping of company data.

Automation

There are many challenges that come with conducting risk management including resource limitations, subjectivity, and the risk of human error. One way to address these issues is through automation. For example, with the use of machine learning, data can be processed and analyzed quickly with no heavy lifting from team members. Automating tasks should reduce the effects of human subjectivity and human error as well.

The automation and standardization of using an assessment Exchange enables you to scale up significantly so you can conduct more assessments and receive more actionable data quickly while using fewer resources.

Collaboration

Whether it's interdepartmental collaboration to ensure that internal TPCRM processes and procedures are followed, collaboration between first and third parties, or collaboration between enterprises when it comes to providing data about cybersecurity practices, it's a key piece to the puzzle of keeping us all safe from continuous cyber threats.

Communication

The more you're able to communicate with stakeholders the benefits of a strong TPCRM strategy, the more likely people will be to adhere to the procedures you've laid out. And when it comes to communicating with leadership about adopting a strategy, being

able to articulate why and how a TPCRM program will help the business grow is an important first step in securing a solution.

Prioritization

Resources — whether time, money, or headcount — seem to be lacking regardless of company size, age, or industry. That's one reason why it's important to utilize a TPCRM solution that gives you the visibility into the risk postures of all your third parties, so you can prioritize remediation strategies to get the most bang for your buck.

Using an Exchange

A cyber risk exchange like CyberGRX is a great place to access the self-attested and predictive risk assessments for thousands of companies around the world. It takes the grunt work out of having to chase down individual third parties to get assessments completed. When you work with an exchange that provides standardized data (and remember, not all do), then you get detailed risk insights that enable you to make rapid, well-informed decisions when it comes to third-party cyber risk.

Regular Security Training and Processes for Employees

We all have a duty to protect our assets, and employees are the first line of defense in preventing mistakes that weaken cybersecurity defenses. These include clicking on links in suspicious emails, opening file attachments from unknown parties, and leaving devices unsecured in public places.

Requiring regular security training for employees is a great way to prevent cyber incidents caused by human error. Regardless of job function, all employees have some interaction with a third party, so it's everyone's responsibility to be educated on threats and remain vigilant. Having well-documented processes in place that help employees validate third-party relationships will also help reduce the risk of team members turning to Shadow IT, which lessens risk even more.

Monitor, prevent, detect, and respond to third-party cyber risks

The landscape of third-party cyber risk management is evolving, driven by increased cyber threats and attacks aimed specifically at third-party providers and supply chain vendors. In order for organizations to effectively protect against these threats, they must focus on cyber-centric data in order to make quick, well-informed decisions.

Third-Party Cyber Risk Management For Dummies provides helpful explanations and practical guidance for rising above compliance to achieve true cyber risk management, turning data into action instead of simply collecting it. Dive in to get started in truly protecting and improving your business.

Inside...

- Explore the evolving threat landscape
- Understand the need for a TPCRM strategy
- Get buy-in from leadership, procurement, and compliance
- Make the most of predictive analytics
- Protect your business from security threats
- Improve business continuity and disaster recovery
- Learn from real-world examples

Cyber GRX

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-88702-7
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.