TPCRM 101

An Introduction to Third-Party Cyber Risk Management

TABLE OF CONTENTS

Part 1

What is Third-Party Cyber Risk Management?

In the cyber sphere, NIST, ISO, AICPA, and DHS are among the multiple organizations that have offered a definition of cyber risk management. While the multiple definitions of cyber risk all differ to a greater or lesser extent, a few key elements remain the same. The universal theme of these definitions is the use of risk measurement to discern the likelihood and damage of events that could negatively impact the confidentiality, integrity, availability, and ownership of cyber assets (including systems and the information they store, process, or transmit) and treating them. Managing third-party cyber risk is an attempt to measure the likelihood and negative impacts of a cyber event that could happen due to the third parties in your ecosystem, and working with those third parties to treat the risk they expose you to.

IN THIS GUIDE, YOU WILL LEARN:

1. Why having an effective and efficient Third-Party Cyber Risk Management (TPCRM) program matters
2. What you need to know to create an effective program
3. How to optimize your current program

Why TPCRM Matters

As organizations increasingly rely on third parties, their ecosystems become larger and more vulnerable to third-party cyber risk. Luckily, there are steps you can take in order to protect your organization from these threats, and ensuring you have a solid TPCRM strategy in place is an imperative first step. (Other actions include utilizing state-of-the-art service providers like Amazon Web Services (AWS) that take a proactive approach to mitigating cyber risks.)

Because unfortunately, more than 60 percent of the breaches in the U.S. can be attributed to third parties, costing organizations an average $7 million – nearly double the cost of an average breach. When you consider the impact to your brand reputation, loss in business, and possible decreases in share value, the overall cost of failing to effectively vet and evaluate third parties is $13 million (Ponemon Institute).

Implementing an efficient, effective TPCRM program is essential to securing your organization's cyber ecosystem by tracking, avoiding, and minimizing the risks that your organization is exposed to. It can also save your organization time and money, while scaling with growth. With a clearer understanding of the cyber risks that your third parties pose, your organization can fine-tune its participation in greater cyber ecosystems, pursuing more opportunity when third-party cyber risk is low, and protecting value when third-party cyber risk is high.

TPCRM and Compliance

The primary objective of cybersecurity is to protect the confidentiality, integrity, and availability of data. In order to be effective, a risk manager needs to know what data their organization processes, transmits, or stores, as well as the sensitivity of that data. Take the time to talk with internal and external stakeholders to classify your data and map that data to where it resides within your ecosystem, including third parties. Because whether you love them or hate them, regulations provide direction that most organizations are required to follow.

It is imperative that you know what regulations are applicable to your organization and industry, and the requirements that those regulations impose on you and any data you collect, process, or transmit. This information will come in handy when determining which third parties to assess, what security controls to assess, and what to do with assessment results. Assessing and managing risk is a requirement for achieving compliance and you can't be compliant without third-party cyber risk assessments.

PRO TIP:

Keep in mind that checking the compliance or regulatory box alone is not a true risk-based approach to third-party cyber risk management. A risk-based TPCRM program will include regulations and compliance, but will go much deeper in terms of pinpointing inherent and residual risk in your ecosystem.

Part 2

How to Create a TPCRM Program

TPCRM Programs Should be Efficient and Effective

Third parties are inundated with assessments and enterprises aren't getting the insights they need – and the cost of failure is high. Third parties spend an average 15,000+ hours completing assessments each year, and the businesses that receive these assessments only take action on 8 percent of them. Approximately 40 percent of organizations use manual spreadsheets and 51 percent employ risk scanning tools to vet their third parties – yet over 54 percent of these organizations say these tools don't provide valuable information.

Without the right tools, you could find yourself relying on possible false-positive information from scans, or outdated data from static spreadsheet assessments – both of which can not only be misleading, but also drain your resources without providing valuable information. Whether you have a TPCRM program in place, or are looking to build one, an effective program should inform decision making throughout the entire process – so you are actually able to identify, prioritize, and reduce third-party cyber risk – and should be able to scale with your needs and ecosystem.

The 6 Steps to Create Your TPCRM Program

Pinpointing and mitigating third-party cyber risks throughout your ecosystem is vital to the security of your organization and requires an effective third-party cyber risk management program. Here's where to start, and what steps to take. Once you know the basics, we'll show you how to optimize your program in a way that'll save both third parties and enterprises time and money while being able to seamlessly scale.

1. Identify Your Vendors

If you are not 100% confident that your organization has on-boarded, vetted, and has absolute accountability for every single third party you are using, we recommend a three-pronged approach:

1. Reach out to Accounts Payable and get a 1-year list of all outgoing payments. We have seen organizations start with a 10,000-line spreadsheet, but within a day or two, carve it down to a manageable 400 payee listing once individuals, subscriptions, and single-payment services were removed.
2. Consult the department that manages legal or contracts regarding your list to see if there are any third parties that have been left off the list, or any third parties with whom your organization's relationship ended prematurely. Additionally, your legal team can help you identify any third parties with which you do or do not have the right to audit.
3. Once these steps are completed reach out to department leads and relationship managers to review and confirm your list.

2. Categorize Your Vendors According to Their Inherent Risk

Develop a brief but succinct scoping questionnaire that can be completed by the owner of the relationship that focuses on the inherent risk of the relationship. Inherent risk is an assessed level of raw or untreated risk – in other words, the natural level of risk associated with a third party without doing anything to reduce the likelihood of occurrence or mitigate the severity of a mishap. Consider limited response questions (yes/no, multiple choice, etc.) to reduce the possible responses and avoid receiving essays. Questions we have seen used in the past:

- Will the vendor process, store or transmit regulated or otherwise sensitive data? (e.g. NPI, PII, PHI, EU Privacy, etc.)
- Where will the service of the vendor be performed? (e.g. on-premises, at vendor location, remote, combination of multiple locations, etc.)
- What is the concentration risk of using this third party? (e.g. no viable alternatives and activity cannot be relocated within a reasonable timeframe or cost, limited viable alternatives and activity could be relocated within a reasonable timeframe or cost, many viable alternatives and could be relocated at an acceptable timeframe or cost, etc.)
- What is the level of regulatory compliance risk associated with the product or service activity? (e.g. High risk – failure to follow prescribed directives may result in substantial fines, restrictions and/or major concerns by regulators, Medium risk – some risk of fines, restrictions and/or concerns by regulators, Low risk – possibility of loss from non-compliance is remote)

3. Develop or Choose a Cybersecurity Assessment

If you choose to develop your own assessment questionnaire you may want to start by leveraging an existing cybersecurity standard. In some cases, your organization may be required to comply with certain standards, which is a great place to start. Some of the more commonly leveraged standards include: ISO 27001 and ISO 27002, NIST SP 800-53, NIST CSF, PCI-DSS, CSA CCM, etc. It is important to identify the controls and control-based questions that are going to provide real value to your organization.

PRO TIP:

CyberGRX automates this step and can immediately reveal inherent risk in your ecosystem with Auto Inherent Risk (AIR Insights™).

However, creating your own assessment tools and questionnaires is like re-inventing the wheel. The CyberGRX Exchange provides the data needed to make an educated and reasonable assessment of risk based on information gained from industry metrics, control effectiveness, risk identification, proprietary analytics, open sources, dark net, etc. As such, CyberGRX helps third-party cyber risk managers identify potential gaps, evaluate process recommendations, and isolate remediation requirements to boost your security posture. And while bespoke assessments may be appropriate for some of your high risk third parties, they often aren't practical for your entire vendor population.

PRO TIP:

Make sure your assessments provide you with actionable data. A structured data set will enable you to run analytics across it to uncover gaps and other information that can inform next steps with your third parties.

4. Conduct Assessments

Start with a plan and establish expectations. Negotiate and set appropriate timelines, with a set start and target finish date for questionnaire completion, evidence gathering, risk identification, report release, and remediation follow-through. Ensure that all parties agree on the scope of the assessment. Ask questions like, "What products or services are in scope?" and "What locations are in scope?" One other consideration is whether or not you have a documented "right to audit" a particular third party.

In some cases, the assessment may consist entirely of a self-assessment questionnaire that your third party will complete. Additionally, you may wish to "validate" the accuracy of your third party's completed questionnaire by requesting that they provide evidence or conduct security control demonstrations.

You may be tempted to opt for onsite security assessments. In reality, onsite assessments are expensive, time consuming, and rarely provide additional insight that cannot be gained from other secure information sharing options, unless:

1. Physical and/or environmental aspects of the assessment are paramount and first-hand observation is mandatory.
2. The third party chooses to retain absolute control of their data.
3. The relationship is new or has had a material change and nature of the service being provided or data being shared with the third party is highly sensitive.

Remember, since your third parties will provide you with sensitive information, it is your responsibility to ensure that throughout the assessment process the assessed organization is confident in the safety, confidentiality, and integrity of the data being shared and that data is only retained if there is a business need to do so and for as short of a defined timeframe as is required.

5. Address Identified Risks

Upon completion of the assessment, including a review of a completed questionnaire and any supplied documentation and evidence to support questionnaire responses, the next step is to put together a report detailing who the third party is, the locations and details of services within scope, and gaps between what the third party has in place and the expected controls necessary to adequately protect any data they are being provided.

The risk appetite of the organization coupled with the scope of the assessment and the sensitivity of the data the third party will receive may dictate the risk treatment, be it acceptance, avoidance, transference or reduction/remediation. If remediation is the chosen path, considerations should be made when working with your third party to create reasonable plans. While policy creation and roll-out should take no more than 15-30 days, capital expenditures (e.g. hardware/software purchases, program creation and development, next generation firewalls, etc.) can take several months to get budgeted, planned, and implemented.

PRO TIP:

A good way to gauge whether your assessments are providing value is if you've actually identified any third parties that create too much risk vs. business value.

6. Continuously Monitor Your Vendors

As long as the relationship remains intact, third-party risk is not going away and there are reasons to continuously or periodically monitor third-party cyber risk, for example, when services expand or decrease, or providers make a material change to their locations or facilities. Re-reviewing the risk associated with the third party or continual monitoring of third-party relationships, controls, and activities are vital for meeting regulatory and compliance requirements, for the health of the relationship and the safekeeping of customer information.

Part 3 How to Optimize Your Program

Reducing third-party cyber risk is without a doubt, a difficult challenge. The thought of gaining visibility into hundreds or thousands of third parties' security postures is daunting – and can be extremely time consuming when using static spreadsheet assessments, or inaccurate if relying on risk scanning tools. Businesses today are demanding a transformational approach that reduces costs and risks from their growing ecosystem of partners, vendors, and affiliates.

In the current heightened regulatory environment, it's no longer sufficient to take a compliance-based approach. Businesses must truly measure and manage risk from their expanding third-party population based on their organizational risk appetite. Longer, spreadsheet-based assessments and hiring more assessors is widely recognized as a poor strategy given today's climate.

So how do you optimize, streamline, and strengthen your TPCRM program?

1. Know what to look for when optimizing
2. Collect and use structured data that allows you to make informed decisions
3. Use an exchange concept to save time, cut costs, and scale
4. Work with vendors who take a proactive approach to TPCRM

What to Look for When Optimizing

As your third-party cyber risk management program matures, you will likely encounter challenges related to resource requirements and timeliness. Risk assessment can be a very laborious and tedious process, particularly if you have large numbers of third parties to assess. Automation is one way to mitigate both resource constraints and lengthy assessment timeframes. You may want to analyze your process to identify any repetitive tasks. These are likely candidates for automation.

No matter how many risk analysts are on your team, you simply cannot be aware of every threat that has the potential to impact your third-party ecosystem. Fortunately, there are countless resources for threat intelligence that can enrich your assessment results and mitigation activities. One use of this type of externally produced data can be to influence the prioritization of corrective actions. You may decide to de-prioritize mitigation if a control weakness is identified during your assessment process, but there is no account of that weakness ever being successfully exploited in the wild.

Collecting and Using Structured Data

Regardless of which assessment standard you choose, it is important to be able to effectively act on the assessment results. Standardization is key to ensuring that assessment outcomes can be analyzed at an enterprise level. Disparate control requirements and assessment questionnaires means that you cannot compare "apples to apples" within your third-party ecosystem. If you are using risk assessments to evaluate potential new third parties, it would be difficult to decide which is the best option using unstandardized data.

PRO TIP:

TPCRM is not a one size fits all strategy. It may make sense to use your own assessment approach on a particular set of third parties and leverage a solution or vendor to handle the rest of your population.

Using an Exchange

Rather than maintaining a one-to-one relationship between companies and third parties, why not use crowd sourced risk assessment information? Organizations complete one validated, comprehensive assessment and share with as many partners as needed, and they can update the information whenever there are changes to their security measures. Businesses request access to these already completed, up-to-date assessments, allowing them to assess more of their third parties, know exactly where risks lie within their ecosystem, and arming them with insights that inform all of their vital risk-based decisions.

An exchange is comprehensive, cost-effective, massively speeds up the process of TPCRM, and can easily scale with your business growth.

PRO TIP:

CyberGRX has created the first and only third-party Cyber Risk Exchange — with over 85,000 (and growing companies on the Exchange. Organizations that have joined have seen a 3x ROI and those benefits will continue to grow.

Part 4 Work with vendors who are proactive

Vendors who take a proactive approach to cybersecurity hygiene are showing their customers that they take the security of not only their own data--but also their customer's data-- very seriously. This helps build trust in business relationships, something that's important when it comes to deciding who to do business with. A great example of a company who has made a point of being very transparent about their security posture is AWS.

Another way third parties can be proactive in their business relationships is by upstream (proctively) sharing any security assessments they have on Exchanges such as CyberGRX. This ensures that customers always have the most up-to-date information on their third parties' security postures, and in the event that there's a cyber threat, precious time can be saved because they'll have that data on hand.

Just remember the basic steps:

1. Have clear goals when creating your TPCRM program, know what regulations you need to adhere to, and keep in mind that a true risk-based approach goes much deeper than compliance.
2. When creating your program, be sure to automate where you can and collect structured data that you can take action on.
3. When optimizing your program, consider an exchange to speed up the TPCRM process, allow you to scale with growth while cutting costs as the same time.

An exchange is comprehensive, cost-effective, massively speeds up the process of TPCRM, and can easily scale with your business growth.

Conclusion

Third-party cyber risk management is a rising concern among organizations of all sizes and in all industries.

Though it can be daunting to address, third-party cyber risk doesn't have to keep you up at night.