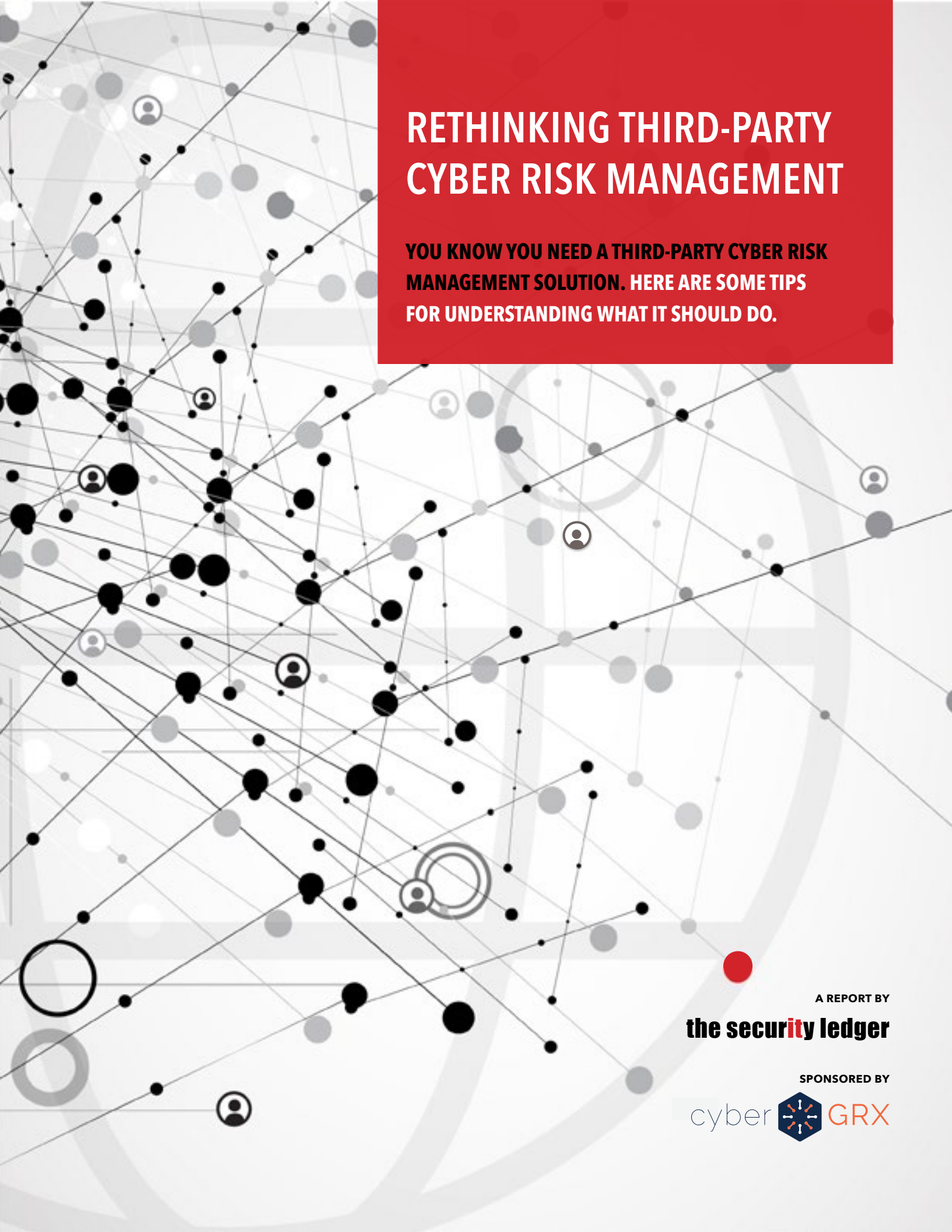


RETHINKING THIRD-PARTY CYBER RISK MANAGEMENT

YOU KNOW YOU NEED A THIRD-PARTY CYBER RISK MANAGEMENT SOLUTION. HERE ARE SOME TIPS FOR UNDERSTANDING WHAT IT SHOULD DO.

A REPORT BY

the security ledger

SPONSORED BY

cyber GRX

CONTENTS

INTRODUCTION

If you've been reading the headlines, you already know that third-party cyber risk is one of the most potent and fast-evolving risks your organization faces. What is the status of your third-party cyber risk management (TPCRM) program? Common in the financial services industry, these are just now making their way into companies in other sectors. Does your firm have such a program? If so, is it working to limit your cyber risk, or is it falling short of the task of keeping you ahead of malicious actors? What are the "must have" features for modern third-party cyber risk management?

The problem of third-party risk and third-party cyber risk are growing and evolving as we speak. This guide will help you better understand the choices before you no matter if your organization hasn't even cracked the seal on third party cyber risk management; has a program, but hasn't updated it recently; or considers itself an expert at third-party risk cyber management. Take the time to review this guide, if only to verify that you are accounting for the many varieties of third-party risk and all the possible solutions out there.

The discussion that follows will help you distinguish a mature cyber risk management practice from an immature one. By the time you complete this guide, you will better understand how you can ensure that your current third-party cyber risk management practices will translate into lower third-party cyber risk and understand where your company's practice sits on the third-party cyber risk management 'maturity curve.'

THIRD-PARTY RELIANCE (AND RISK) IS GROWING

Third Parties Pose Significant Risk to your Business

Just scanning the headlines of your local paper tells the story. Consider, for example, the fate of the firms LabCorp and Quest Diagnostics, which in 2019 disclosed massive data breaches affecting around 20 million patients. The source of the breach: the American Medical Collection Agency (AMCA), a medical collections firm. And that's not the only example. Some 15 million health records were exposed in 2018 as a result of attacks on electronic health record systems used by a large number of hospitals and health systems.[1] Outside of healthcare, e-commerce sites across industries have been the victim of so-called "Magecart" skimming attacks that place malicious scripts on compromised websites that can siphon off sensitive transactional data like credit card numbers. In one such attack, more than 200 online stores belonging to universities in the U.S. and Canada were hacked[2] after the compromise of a single e-commerce platform, PrismWeb, made by the firm PrismRBS.

There is, of course, a third party component to one of the most devastating and costly malware attacks ever: NotPetya (aka "Nyetya") had roots in the compromise of a software update service used by M.E.Doc, a Ukrainian finance software package.[3]

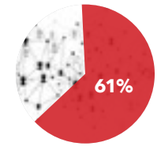
The growth in third-party compromises tracks to the private and public sector's growing reliance on third parties of all sorts. This includes traditional suppliers, vendors and subcontractors as well as resellers and distributors, business partners and affiliates. Surveys of both private and public firms find that third-party relationships often number in the thousands or even tens of thousands, depending on the industry. A senior compliance lead at a large pharmaceutical firm interviewed for this report said her company tracked "tens of thousands" of suppliers globally. "You're seeing what's happening in the market with other companies being breached and you understand the potential impact," she told us.

Business and technology trends are boosting the reliance on third parties, as well. The phenomenon that McKinsey calls the "digitization" of industries sees more companies turning to managed service providers (MSPs) and cloud services firms to provide key corporate functions.[4] In just one measure of this phenomenon, the Technology Services Industry Association (TSIA) notes that, for the largest 50 technology firms, services accounted for just 41% of total revenues in 2008 ($318b), but jumped to 55% ($456b) in 2018, while product revenues have declined.[5]

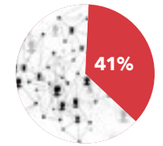
[1] https://www.healthitsecurity.com/news/15-million-patient-records-breached-in-2018-hacking-phishing-surges
[2] https://www.zdnet.com/article/hackers-steal-card-data-from-201-online-campus-stores-from-canada-and-the-us/
[3] https://blog.talosintelligence.com/2017/07/the-medoc-connection.html
[4] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/five-fifty-the-digital-effect
[5] https://www.tsia.com/resources/the-state-of-managed-services-and-xaas-2019

Cyber Risk Grows with Third-Party Reliance

Outsourcing internal functions to third party providers gives a boost to productivity and can reduce operating costs. But heavier reliance on third parties increases your company's attack surface, making it more vulnerable to cyber attacks. For example, a 2018 survey of more than 1,000 CISO and security and risk professionals in the U.S. and U.K. found that 61 percent of their companies faced a data breach because of a vendor or third party. Even more worrying, more than a fifth of those surveyed security and risk professionals said they did not know if their employer had experienced a third-party data breach during the past 12 months.



61% of companies faced a data breach because of a vendor or third party.[6]



Of 2,410 U.S. based IT and IT security practitioners reported that 41% of third parties had misused or shared confidential information with other third parties.[7]

59% of CISOs report that their organization had been the victim of a third party breach.[8]

THIRD-PARTY BREACHES

Data breaches linked to third parties are a growing problem. Here are recent incidents involving compromises of third-party providers.

EAT STREET

In June, the food ordering service EatStreet notified restaurants, consumers and food delivery services that a hacker had penetrated its network and made off with customer data. The breach was carried out by a hacker who claimed to have taken information on as many as six million individuals.

ASCENSION

Tens of thousands of consumers who applied for loans through major banks including Citigroup, HSBC, Wells Fargo, CapitalOne and even the Department of Housing and Urban Development had sensitive financial information exposed when Texas based data analytics firm.

AMERICAN MEDICAL COLLECTION AGENCY (AMCA)

A provider of billing services for health-care firms including Quest Diagnostics and LabCorp, AMCA was compromised by hackers between August 2018 and March 2019. Private health information on more than 20 million U.S. patients is believed to have been stolen.

CLICK2GOV

A compromise of Click2Gov, which provides online payment services to municipalities across the U.S. has resulted in the theft of more than a quarter million payment records in 46 U.S. cities. The records have been pawned on the dark web, netting criminals millions, according to Gemini Advisory.

[6] https://www.pymnts.com/news/security-and-risk/2018/third-party-data-breaches-cybersecurity-risk/
[7] "Measuring & Managing the Cyber Risks to Business Operations," Ponemon Institute
[8] https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Res ults-2018-Third-Party
[9] https://www.zdnet.com/article/eatstreet-food-ordering-service-discloses-

ASSESSING THIRD-PARTY CYBER RISK MANAGEMENT MATURITY

Strict data privacy and security regulations that have emerged in recent years have imposed substantial fines on companies found mishandling sensitive data. That means that, for companies holding onto personally identifiable information, the cost of ignoring third-party risk is growing.

Regulations like the European Union's General Data Privacy Regulation (GDPR), California's Consumer Privacy Act and New York State's Information Security Breach and Notification Act have increased the risk and potential cost of holding onto personally identifiable information for a wide range of firms.[10]

EFFECTIVE?

Companies spend an average of $2.1 MILLION annually vetting third parties. Of 600 IT professionals surveyed by The Ponemon Institute, MORE THAN TWO THIRDS said the processes they use to vet third-parties are only SOMEWHAT EFFECTIVE or NOT EFFECTIVE AT ALL.[11]

Third-Party Cyber Risk Management Red Flags

Across industries, high costs and limited scale characterize third-party cyber risk management programs. As a result, many have languished, even as the need for them has grown. Absent robust tools to manage their third-party relationships, organizations are struggling to scale inefficient processes to meet the new demands of regulators and business partners for third-party risk assessments. How do you know whether your current third-party risk and third-party cyber risk management practices are mature or immature? Below, we've included some "red flags".

Lots of Buck, Very Little Bang

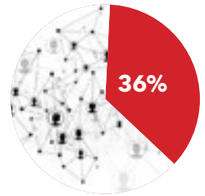
Spending a lot on third-party risk management with little to show for it is perhaps the best indicator that your TPCRM processes need to be re-evaluated. Among other things: consider how much you're spending on assessments compared with what percentage of vendors are covered by them.

Devils You Know

Immature third-party cyber risk management programs typically address only a portion of an organization's third-parties, and often not the vendors who pose the greatest risks.

Consider how many vendors your current TPCRM program covers and whether the vendors covered are those that pose the highest risk to your organization. Spending handsomely to achieve a small reduction in risk is rarely advisable. Also consider how many full- and part-time cyber risk analyst positions you're supporting simply to validate vendor responses.

[10] Center for Financial Professionals: "Third Party Risk: A Journey Towards Maturity"
[11] "The Cost of Third Party Cybersecurity Risk Management," Ponemon Institute



The Ponemon Institute's survey of 600 IT risk professionals found just 36% of respondents said manual third-party assessment tools were "highly effective" in vetting third parties security protection capabilities.

Static Assessments, Fluid Risks

A recent Ponemon Institute survey of 600 IT risk professionals found 40% use mostly manual procedures like spreadsheets to assess third-party risk, but just 36% of respondents said such assessments were "highly effective" in vetting third parties security protection capabilities.

Given the limitations of such tools, an over-reliance on cumbersome spreadsheet-based questionnaires should be considered a "red flag" that your TPCRM program needs to modernize.

Threat- Not Risk-Focused

Immature third-party cyber risk assessments may treat cyber threats discreetly: noting the presence or absence of specific controls for specific threats. Alas, when it comes to cyber risk, the whole is more than the sum of its parts. Consider whether your TPCRM program is focused on cyber risk above and beyond discrete threats or attack vectors.

Ideally, third-party cyber risk assessments understand the inherent risk posed by a vendor (the risk absent any controls), identify the controls used with that vendor and spot gaps in those critical controls that might impact your risk posture.

Not Verified

Legacy or immature third-party cyber risk management programs often lack the ability to verify the findings of risk assessments. The findings of automated scans and manual assessments are a good starting point in grappling with third party cyber risk. But tools and services must be in place that enable first party firms to verify the accuracy of the information about security controls and procedures.

Mature third-party cyber risk management offerings should offer some form of risk verification for high-value vendors. Those might come in the form of audits of vendor self assessments, remote or on premises independent assessments, red team engagements, or all of the above.

RETHINKING THIRD-PARTY CYBER RISK MANAGEMENT

As we noted, the last ten years has seen the issue of third-party cyber risk move from the data center to the C-Suite and the board room. A number of important advancements and tools for third-party cyber risk management warrant attention as you look to stand up a TPCRM function within your organization or to revamp established processes. Here are some pointers you should consider as part of your due diligence:

Think Beyond Compliance

Compliance with industry or government regulations is a top concern, naturally. But third-party risk goes far beyond mere regulatory compliance. As a risk manager at one leading global investment firm noted: third-party cyber risk management began more as a compliance check box due to regulations such as Sarbanes Oxley, SEC OCIE, FINRA, etc. It has evolved into an instrumental practice for ensuring the security of his firm.

"Companies rely more on third parties and those third parties are being given more and more data, but do not always have security programs commensurate with the data they manage," he noted. "Still, a breach of a third party becomes a breach of your company as it relates to data loss, reputation loss and financial loss."

Similarly, the compliance lead at a major pharmaceuticals firm said that her employer's decision to stand up a third-party cyber risk management function was rooted in concerns about HIPAA compliance, but also in recognition of the changing threat landscape and the value of patient health information to malicious actors.

"It is becoming more important to holistically look at vendor risk," the risk manager at the global investment firm observed. *"A point-in-time control assessment of the vendor's program is not enough anymore. You should be evaluating what the business use case is, the end to end flow and integration of this vendor in your environment, and more importantly how to securely configure the product. With SaaS being the new trend, if the vendor has a strong security program but you incorrectly configure the product or tool, you are still at risk."*

Move Beyond Risk Ratings

In recent years, third-party risk rating services have cropped up, offering an alternative to bespoke, in-depth assessments. These automated scanning services take a "hacker's eye" view on an organization: providing fast and continuous monitoring of potential risks, however the results include many false positives and can be misleading. These services look for risk indicators such as outbound traffic to malicious hosts or other signs of infected machines on company-owned or operated infrastructure. Based on the findings of these automated scans, third-party scanning services offer credit score-like cyber risk ratings of third-party firms: positive findings effect risk scores as do improper configuration of security controls or other evidence of lax security behavior.

Today, many organizations now rely on risk rating services as a component of their TPCRM programs. In its survey, The Ponemon Institute found that risk scanning tools were the most common form of assessment tool organizations used to measure third-party risk.[12]

While these automated services can be helpful, they are not sufficient to determine third-party risk alone. Depending on how they are configured, third-party cyber risk scanning services might overlook key risk indicators or trip over "false positive" indicators in ways that can mislead a customer about the true cyber risks it faces. If nothing else, the mixture of factors that contribute to risk scores varies from vendor to vendor, as does the method by which risk ratings are calculated. Practically, that means third-party risk scans, taken alone, are of limited utility and risk missing critical security issues or trumpeting low-level risks.

Use Risk Data to Take Action

Identifying the risk is just half of the battle. Security and IT leaders also need to act upon the data they have: implementing new controls or processes or adjusting third-party relationships to mitigate the identified risks.

Reports that talk about vulnerabilities in third-party infrastructure that have been identified and patched are useful. But C-suite and board members want to understand the bigger context: are risk management efforts improving the organization's risk posture? Is the organization more or less vulnerable to an adverse cyber incident than it was last month?

The key to making data actionable is to cultivate high quality and structured assessment data. This is harder than it may seem. As we noted earlier: bespoke assessments often yield reams of data that are difficult to structure and correlate, while third-party risk scans may feed you information that is unreliable or not actionable.

Once you have assessed your third parties, does your TPCRM solution help you identify which vendors pose the greatest risk and require immediate attention? Does it provide you with the tools and data that you need to "tell a story" about an organization's third-party cyber risk efforts? Your TPCRM solution should help you to turn risk data into concrete mitigation actions.

Prioritize Third-Party Risks

As we noted above: even where third-party cyber risk management programs exist, they do not cover all of a vendor's actual third parties. Often, that's due to a lack of resources (staff) and the difficulty of scaling what are still highly manual on-boarding and assessment programs. After all, for companies with hundreds or thousands of third party providers, it is not realistic or even appropriate for first parties to apply the same due diligence for every

[12] https://www.cybergrx.com/ponemon-third-party-cyber-risk-management-report/

firm. Informed decision making needs to start at the very beginning by assessing your entire ecosystem and, from that, identifying the vendors that pose the most risk.

Know Where to Start

The first step in building a robust third-party risk- and cyber risk management function, then, is to develop a system of identifying and tracking all your third-party vendors. Start by listing all the vendors that you know about. That may be vendors you have interacted or corresponded with, providers of tools and technologies and services you know your company uses and so on. Go through the same exercise with other team leaders to "crowd-source" a list of known vendors and expand the list of known third party entities that your organization interacts with.

Overwhelmed at trying to track down all your third-party vendors? Your accounting department is a great place to start looking for third-party relationships that may have escaped your notice. Ask your accounting department to give you a list of all outgoing payments for the past 12 or 18 months (dollar amounts aren't important). That will provide you a nearly comprehensive (albeit noisy) list of vendors the company works with.

Consider that large and diversified vendors and consulting firms might have multiple relationships with your organization - each representing a different level of risk, said Jonathan Ehret of the Third Party Risk Association. Similarly, seemingly low level vendors might pose a greater risk than you would assume. *"You might have a vendor who prints your company logo on pens, so you look at them as super low risk, but they might have your entire customer list or other (personally identifying information),"* said Ehret.

Finally, use your knowledge about the interactions between your organization and its third parties to identify your highest risk third parties. The "Big Four" accounting firm that manages your company's financial reporting and compliance has much deeper, more valuable and high risk connections to your organization's network and IT environment than the sandwich shop that delivers catering for lunch. Vendors who have remote access to your corporate network or receive sensitive intellectual property or customer data pose a greater risk and should be the focus of more in-depth assessments, engagements and remediation efforts, where necessary.

Understand and Identify Inherent and Residual Risk

Adding to the challenge of third-party cyber risk management is the fact that any third party can potentially pose a risk to your organization. HVAC systems, cloud application providers - even local charities have all been used as avenues of opportunity and attack.

That is why it is critical to understand the inherent risk of all your third parties. Calculating the inherent risk a third party poses requires you to identify a use case for each third party, and understand how much risk they create for you in their natural state (with no security in

place). Inherent risk can help your organization decide up front what that relationship will look like, how much and what kind of information exchanges will take place and how much scrutiny to pay to the cyber security of a new- or existing partner.

Without a tool to help you, it can be time consuming to calculate inherent risk. Still, it is absolutely critical to do so, as an understanding of third-party inherent risk informs the rest of your TPCRM strategy. It sets a baseline you can use to assess, measure and report on. Thankfully, the industry is catching on to this and new solutions are coming to market that help automate the determination of inherent risk.

In addition to understanding the inherent risk that your third parties pose, you also need to determine the residual risk of each of those vendors. Residual risk refers to the risk posed by third parties after accounting for security controls and other mitigation efforts. It is the truest measure of the risk a party poses to your organization.

Understanding residual risk requires a deeper analysis of a third partys' environment than automated scans can provide. That may include on-site or remote assessments by trained professionals to validate the existence of security controls across a number of control areas - not just core IT functions and operations, but also management, strategic planning, regulatory compliance and so on. Furthermore, security controls need to be mapped back to existing frameworks such as NIST 800-53 v4, ISO 27001 so that control gaps can be identified and addressed.

Shine a Light on Shadow IT

The advent of so-called "shadow IT" systems on enterprise networks complicates third-party risk assessments. Often, such tools and services are adopted ad-hoc at the department or even group level. They may not be managed by your organization's IT group - or even visible to it. In terms of identification, these services may be paid for directly by an employee, rather than through traditional IT procurement channels, making them more difficult to surface in an audit.

Special effort must be paid to ferret out shadow IT applications and technologies and add them to your list of third parties. Surveys or interviews with team leads and individual employees may be needed to identify shadow IT technologies and services that are in use within your organization.

Data Access a Key Consideration

For cyber risk management, you will want to ask third parties about what kinds of data your organization shares with them. Do they collect regulated data such as personal health information (PHI), credit card or bank account numbers, personally identifying information (PII) and so on? If so, that increases the risk they pose to your organization and warrants further assessment.

THIRD PARTY RISK FRAMEWORKS

NIST 800-53 and NIST 800-171 offer detailed guidance to security risk management practices for both Federal (-53) and non-Federal (-171) systems. Both offer guidance on acceptable controls based on low, medium, or high risk ranking vendors and third parties.

ISO 27001

A privacy focused extension to the ISO 27000 series, ISO 27001 is closely aligned with the EU's GDPR. It also includes specific instructions on managing third party supplier risk as part of Annex A of the standard.

NEW YORK STATE 23 NYCRR 500

Designed specifically for financial services firms operating in New York State, 23 NYCRR 500 contains detailed guidance for assessing the security of third party providers that handle sensitive financial information.

Also: you will want to determine whether they have access to any part of your network and by what means: VPN, web application, direct network connection, and so on. You will want to ask about how your data is transmitted to and from their environment and how it is stored on their IT assets and for how long.

Vet and Validate Your Third Parties

Equipped with a comprehensive database of your third-party providers and a baseline understanding of those providers' inherent risk, you are ready to go deeper: assessing your organization's relationship with each of your vendors and validating the security of high value and high risk third parties.

This step is the most critical and potentially time consuming for your business. However, without a good assessment of your third-party vendors, you will struggle to accurately manage your cyber risk.

The experts we spoke with described various methodologies for assembling this assessment. Most recommended using third-party risk frameworks such as NIST 800-53 Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations"[13] and ISO/IEC 127001[14] as a foundation.

To validate third-party compliance with these methodologies or with your organization's bespoke assessment, you may need to enlist the services of an experienced auditor or management consulting firm with expertise in IT audit and compliance.

Rank and Repeat

The risk professionals we spoke with all ranked their third-party providers in some way. The exact makeup of these tiers is less important than that they exist. However, the risk experts and executives generally agreed that ranking vendors, prioritizing your response based on those rankings and frequently reassessing your third-party vendors was critical.

[13] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
[14] https://www.iso.org/standard/54534.html

Generally, they divided vendors up into “high,” “medium” and “low” risk. Don’t over-read risk rankings. Middle tier firms may pose a significant risk to your organization, with access to sensitive data, networks or IT assets. However, these vendors do not pose an immediate risk to business operations and business continuity. These vendors warrant thorough analysis and vetting to assess their cyber risk and existing controls. They may or may not require a separate first-party validation of security controls.

Lower tier firms may pose no immediate risk to your organization because they do not handle company data or have access to company networks or IT systems. By virtue of their relationship to your firm, these lowest tier third parties still warrant an assessment, but one that is more limited in scope and may be limited to a vendor self assessment along with an independent third-party risk score.

Monitor Continuously

One limitation of traditional point in time third party assessments is that they fail to keep abreast of the fast-changing cyber risk landscape. Third-party cyber risk exchanges provide a means of doing continuous risk monitoring. Automated third-party cyber risk scans can capture changes to a firm’s risk posture and alert first parties of the shift in the risk profile of their partner in real time.

With adequate warning, first-party organizations can leverage dynamic assessments to look deeper at a third party, identifying meaningful changes to its risk posture that could be the precursor to an attack or compromise.

HIGH RISK VENDORS

The highest level risk rating is applied to organizations deemed “business critical” and without whose services your organization could not function.

MEDIUM RISK VENDORS

Middle tier firms may also pose a significant risk to your organization, with access to sensitive data, networks or IT assets, but do not pose an immediate risk to business operations.

LOW RISK VENDORS

Lowest tier firms may pose no immediate risk to your organization because they do not handle company data or have access to company networks or IT systems.

1

2

3

Prioritize Efficiency and Scale with Third-Party Exchanges

Given the trend towards larger ecosystems of third-party providers, any third-party cyber risk management platform needs to address efficiency and help organizations scale to meet the increasing demand for third-party cyber risk assessments. That’s why recent years have seen the emergence of third-party cyber risk exchanges.

Exchanges Address Scale and Cost

FIRST: third-party exchanges provide a shared platform for aggregating third-party cyber risk assessments.

SECOND: exchanges provide a solution for the high cost of third-party cyber risk management by aggregating cyber risk assessments and distributing the cost of assembling them across a broad population of first parties.

THIRD: third-party cyber risk exchanges offer a standardized approach to evaluate the business exposure and cyber risk that third party vendors’ pose to your business.

Using automated third-party risk scans and first party-provided vendor profile information, an “inherent” vendor risk level is determined based on factors such as their access to sensitive or regulated data, remote access to your network or the details of the third-party’s public Internet “footprint.”

Inherent risk scores provide a useful measure to prioritize further third-party risk assessment activities ranging from intensive, in-person assessments to independently validated remote third-party assessments to vendor self-attestation for the lowest risk third-party providers.

Additionally, exchanges streamline and ensure consistency in the administration of risk assessments. The exchange takes on the task of onboarding new third parties and eliminates redundancy on the part of both first and third-party vendors as it relates to onboarding. One-off, per-vendor assessments are replaced with shareable assessments that can be accessed by multiple first parties via the exchange, greatly lowering the cost to the parties and increasing the efficiency of the assessment.

Finally, exchanges open the door to data analysis and machine learning tools, which can glean insights from across third party vendor profiles: identifying and prioritizing control gaps found in assessments and providing first parties with insights into residual risks to their organization that are the foundation of remediation efforts and investments.

TALKING THIRD-PARTY CYBER RISK TO THE C-SUITE

Obtaining the backing of senior executives and the board is a critical and overlooked step in building a mature, third-party cyber risk program.

Third-party cyber risk management is a long term investment and one that transcends any particular service or tool. It is an endeavor that requires a 'whole of company' commitment and the continued attention, support and engagement of company executives, who will provide the resources to staff and equip your TPCRM program and help direct the program to best meet the organization's needs.

The experts we spoke to observed, darkly, that a data breach or adverse cyber event is often the most effective tool for revealing the gaps in an organization's current approach to cyber risk management. After all: a third-party breach communicates like nothing else the need for a third-party cyber risk management program to executives and the board.

That said, no company wants to invite such misfortune. You want to make the business case for third-party cyber risk management not in the midst of a crisis, but when cooler heads reign. Leaning on data is a good place to start on the road to winning board approval for third-party cyber risk management.

1

Making the Case for TPCRM

FIRST: senior IT security and risk officers (CSO, CRO) should take opportunities to underscore the growing threat of third-party risk and its connection to major, adverse cyber incidents within your industry or the broader economy.

2

SECOND: risk management pros need to "connect the dots" between headline-grabbing breaches and an organization's known and unknown risks - even when the incident isn't directly translatable (i.e. same industry, same platform used, etc.)

A major data breach linked to insecure cloud storage repositories might become an occasion to remind executives and the board about an organization's own cloud risk and the need to better assess its myriad third-party relationships with cloud providers. A story about a sophisticated hacking group leveraging access to managed services provider networks to attack their customers is a great launching point for a discussion of the need to closely manage the third-party cyber risk of critical business partners.

If all else fails, remind executives and the board that - fair or not - they are held responsible and accountable should a breach occur. That is true whether or not they consider third-party cyber risk their problem. In just one example of this, a survey of members by the Center for Financial Professionals found that four out of five respondents put responsibility for third-party risk at the C-suite and board level, either with the Chief Risk Officer, Chief Executive Officer or others.[15] We've already discussed the material and reputation costs imposed on companies that fail to address third party cyber risk. Executives need to understand that their reputation and even their jobs are on the table as well. It will be your job to convey that message and convince them of its truth.

[15] Center for Financial Professionals: "Third Party Risk: A Journey Towards Maturity"

CONCLUSION

Despite the rash of news and incidents related to third-party compromises, many organizations and even entire industries are still at the very early stages of assessing their exposure to third-party risk, including cyber risk.

Today, the tools and processes that many organizations rely on to manage third-party cyber risk are inefficient and error prone. The next ten years will bring about a sea change in how companies across the economy address this critical category of risk. New approaches like cyber risk exchanges, advanced analytics and better data will allow organizations to closely monitor and manage the cyber risk of even thousands of individual providers.

Developing your third-party cyber risk management program is an iterative process. You will need to work over time to both expand the reach of your third party cyber risk management program, and address outstanding issues with your third-party providers, or alter your relationship accordingly.

At the most senior levels of your company, the engagement with third-party cyber risk management needs to be iterative as well. Senior executives and board members will need to be kept abreast of third-party cyber risk management efforts, the organization's risk posture and the impact of third-party cyber risk on strategic planning. Time should be given to articulate and understand the organization's appetite for cyber risk and how that may bear on its relationships with current or future third-party providers.

Finally, your organization should look for opportunities to leverage cutting edge third-party cyber risk management tools and platforms, including third-party cyber risk management exchanges. These can provide a means of accelerating and streamlining the third-party cyber risk management process, while also lowering its overall cost to your organization. Risk exchanges are one example of a recent development that provides powerful tools and insights to help executives and board members understand their options and reach decisions regarding third-party providers that are in the long term best interest of your organization.

ABOUT US

CyberGRX provides enterprises and their third parties with the most cost-effective and scalable approach to third-party cyber risk management today. Built on the market's first third-party cyber risk Exchange, CyberGRX arms organizations with a dynamic stream of third-party data and advanced analytics that help organizations efficiently manage risk in their partner ecosystems. Based in Denver, CO, CyberGRX was designed with partners including Aetna, Blackstone and MassMutual.

For more information, visit www.cybergrx.com

The Security Ledger is an independent security news website that explores the intersection of cyber security with business, commerce, politics and everyday life. Security Ledger provides well-reported and context-rich news and opinion about computer security topics that matter in our IP-enabled homes, workplaces and daily lives.

Founded in 2012, The Security Ledger has been recognized for breaking coverage of security-related issues, including leading edge coverage of security as it relates to The Internet of Things. It has been voted a Top 100 Information Security Blog in 2017. Security Ledger stories regularly appear on the front page of Slashdot.org, as well as Reddit, Techmeme, and other leading technology news sites. We have also been recognized by leading industry publications for our pioneering work as an editorially independent, privately sponsored news website.

ABOUT THE AUTHOR

Paul Roberts is the publisher and Editor in Chief of The Security Ledger, an independent security news website that explores the intersection of cyber security with the Internet of Things. Paul is a seasoned reporter, editor and industry analyst with more than 15 years' experience covering the information technology security space. His writing about cyber security has appeared in publications including The Christian Science Monitor, MIT Technology Review, The Economist Intelligence Unit, CIO Magazine, ZDNet and Fortune Small Business. He has appeared on NPR's Marketplace Tech Report, KPCC AirTalk, Fox News Tech Take, Al Jazeera and The Oprah Show.

Prior to launching Security Ledger, Paul worked as a Senior Analyst in The 451 Group's Enterprise Security Practice. He has held positions as a senior writer and editor at noted industry publications including Threatpost, Infoworld and eWeek and The IDG News Service. You can find Paul online on Twitter (@paulfroberts, @securityledger, @secthings) and on http://www.linkedin.com/in/pfroberts/.

www.securityledger.com