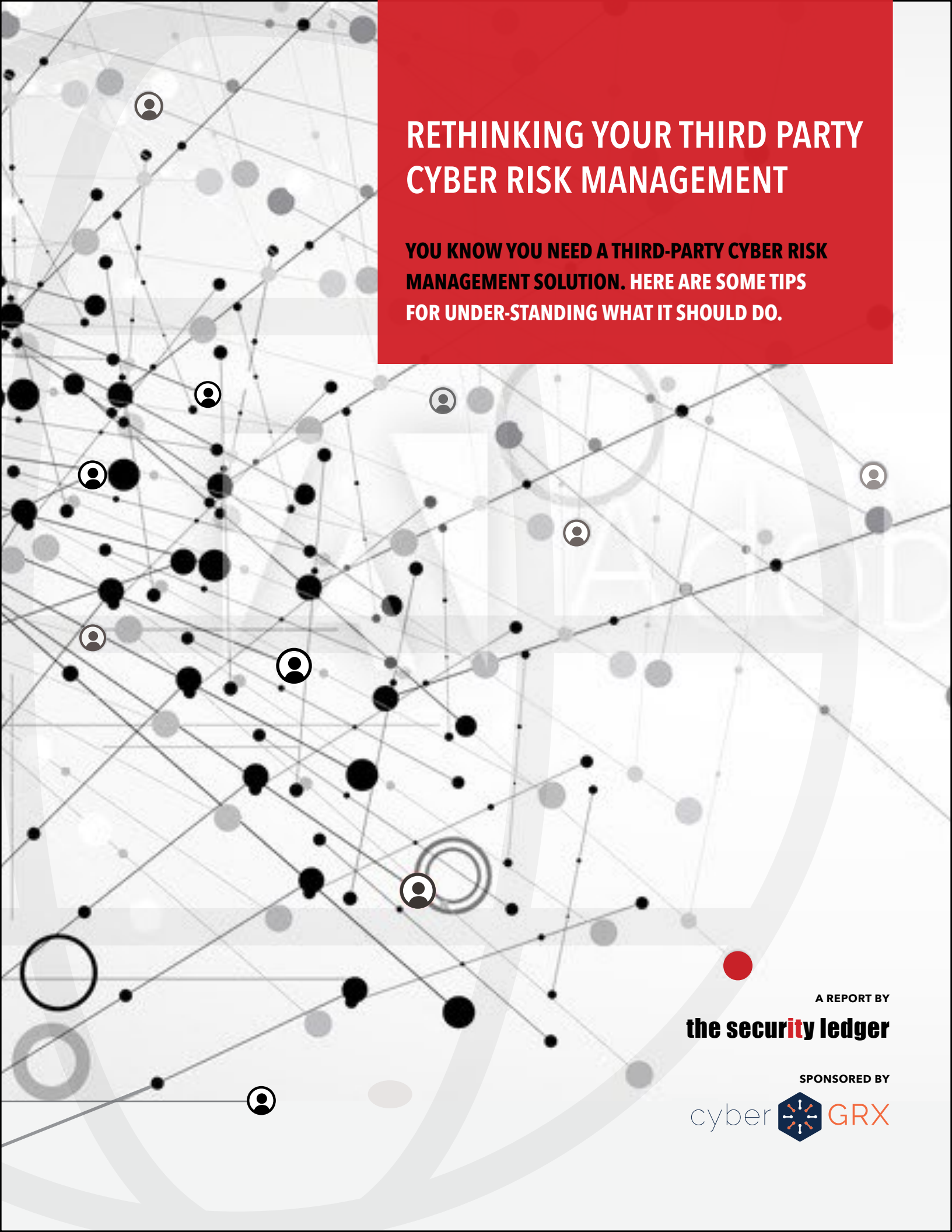


RETHINKING YOUR THIRD PARTY CYBER RISK MANAGEMENT

YOU KNOW YOU NEED A THIRD-PARTY CYBER RISK MANAGEMENT SOLUTION. HERE ARE SOME TIPS FOR UNDER-STANDING 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?

Why publish this guide? Because 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

Your business partners, suppliers and other 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]

Thousands of Third Parties

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.

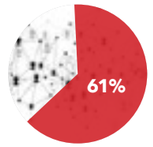
Business and technology trends are boosting the reliance on third parties, as well. The phenomenon that McKinsey calls the "digitization" of industries sees more companies turning to managed service providers (MSPs) and cloud services firms to provide key corporate functions.[4] In just one measure of 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

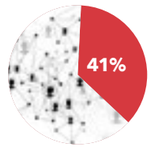
2018 survey of more than 1000 CISO and security and risk professionals in the U.S. and U.K.

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 a third party their organization relied on had "misused or shared confidential information with other third parties.[7]

A 2018 survey found 59% of CISOs reporting 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.

CAPITAL ONE

Paige Thompson, an employee of Amazon.com is accused of stealing data on 100 million U.S. customers of credit card firm Capital One. Thompson is also believed to have abused her position to steal terabytes of data from more than two dozen other companies.

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

ASSESSING YOUR CYBER RISK MANAGEMENT MATURITY

In just one example, the hotel chain Marriott was fined £99 million ($123 million) in 2019 under GDPR for a 2014 breach of a reservation system at the hotel chain Starwood that affected 339 million customers. Marriott acquired Starwood in 2016. In a statement accompanying the fine, UK Information Commissioner Elizabeth Denham said that GDPR's protections for personal data mean that companies must "carr(y) out proper due diligence when making a corporate acquisition, and pu(t) in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected."[10]

Despite the increase in exposure, third-party cyber risk management practices vary greatly across companies and industries. Even in the financial services and insurance industries, one survey found that two-thirds of third-party cyber risk management programs are immature: lacking a solid grasp of inherent risk and well-defined risk appetites.[9] In healthcare, oil and gas or the public sector, recognition is just dawning of the need for a distinct third party risk management function. Third party risk management and third-party cyber risk management practices in these industries are far less common.

Regardless of your industry and whether third-party cyber risk management practices are new or well established at your firm, you want to make sure that those practices are effective, timely and actionable. You want to move your third-party cyber risk management practices along, down a maturity curve from cursory to comprehensive; from periodic to continuous and from informational to actional.

A fast-growing Cost Center

Third party exposure is a growing cost center for organizations. The emergence of strict data privacy and security regulations in recent years including the European Union's General Data Privacy Regulation (GDPR), the California Consumer Privacy Act, the New York State Information Security Breach and Notification Act 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.

Marriott is hardly the only company (or even the only hospitality company)[11] to suffer from a third party breach. Absent robust tools to manage their third-party relationships, organizations of all kinds are struggling to scale inefficient processes to meet the new demands of regulators and business partners for third party risk assessments.

[9] **Center for Financial Professionals:** "Third Party Risk: A Journey Towards Maturity"
[10] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/
[11] https://www.sabre.com/insights/releases/sabre-update-on-cybersecurity-incident/

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.[12]

Security Ledger interviews with IT risk professionals echoed this. An information security and risk executive we spoke with at a leading investment firm said that his company had been spending upwards of $600,000 a year to support a bespoke third-party cyber risk assessment program that still failed to cover the majority of his firm's vendors. Inefficient and manual processes were one reason for the high cost and limited scope of the program, including administering spreadsheet-based questionnaires and retaining full time cyber risk analysts to validate vendor responses.

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.

Snapshots, Checkboxes and Customization

In conversations with leading risk and security professionals about their third-party cyber risk practices, we noted that many described legacy programs focused on regulatory compliance and paper-based or online questionnaires. *"Ten or 15 years ago (third-party risk management) was basically a Word document with questions that got sent out,"* says Jon Ehret the President and Co-Founder of the Third Party Risk Association.[13] At many organizations today - particularly those that are not far down the road of third-party cyber risk management, static questionnaires and checkboxes are the norm, he says.

Static Assessments, Fluid Risk

When performed correctly, ~~static~~ assessments are a powerful element of a third party cyber risk management. However, assessment tools used by many organizations are in need of an upgrade.

The Ponemon Institute survey of IT risk professionals found 40 percent use mostly manual procedures like spreadsheets to assess third parties. The problems that go along with these tools are well known. For one: assuming they are accurate, questionnaires are still static: capturing a moment in time: the state of affairs when the questionnaire was administered. Cyber risk, on the other hand,

[12] "The Cost of Third Party Cybersecurity Risk Management," Ponemon Institute
[13] https://www.tprassociation.org/

is fluid: changing on a daily or even hourly basis depending on factors such as the disclosure of software vulnerabilities or the actions of shadowy online hacking and cyber criminal groups. An annual compliance questionnaire completed the day before the group The Shadow Brokers dumped a cache of highly potent hacking tools and Windows vulnerabilities like EternalBlue in April, 2017[14], might have deemed a company's third parties to be hardened against attack. A day later, their security was known to be at risk, but the changing risk environment would not make it into that point-in-time assessment.

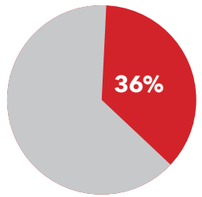
Drowning in (Unstructured) Data

Additionally, assessment tools produce reams of unstructured data in either electronic or paper form that then must be digitized, parsed, structured and sanitized before it can be analyzed and mined for actionable insights. This extra step, if it's even taken, can encumber your organization's third-party cyber risk management process.

The overhead created by manual third-party assessment tools may explain why they often fail to meaningfully improve security at organizations that use them. The Ponemon Institute's survey of 600 IT risk professionals found that just 36% of respondents said such assessments were "highly effective" in vetting third parties security protection capabilities.

This overhead of third-party cyber risk assessments is worth considering as many organizations invest time and resources creating customized assessments for their vendors. While such risk assessments have a benefit, customization is a double-edged sword; the more specific your assessments, the harder it will be to apply them across a wide range of vendors to achieve a broad understanding of your risk posture or conduct "apples to apples" risk comparisons.

That is why, third-party cyber risk assessments (customized or not) often become an end in themselves: a task to be checked off a list not a tool to reduce third-party cyber risk exposure. In this way, bespoke, manual assessments can actually impede your TPCRM program.



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

[14] https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

Silent Scream: The Downstream Effects of Assessments on Third Parties

It's also worth considering the burden customized assessments place on third parties, especially as the use of third-party cyber risk assessments grows across industries. In just one measure: Ponemon's survey of IT risk professionals found that respondents in the financial services sector reported spending more than 17,000 hours annually completing third-party assessments. Respondents in the retail sector were only slightly behind that, reporting an average of more than 15,000 hours annually.

Digging into the data, despite spending the most time completing third-party assessments of their cyber security practices, both sectors still had a higher than average likelihood of suffering a third-party breach, based on the sample of respondents. In other words: the extra time spent completing assessments didn't translate into improved security for these organizations. The truth is that the overhead of completing such questionnaires at scale is proving to be a major drain on the productivity of third-party IT risk teams. Time spent completing similar, bespoke assessments comes at the expense of tasks that could actually improve their organization's security posture!

The Devil(s) You Know: Limited Vendor Coverage

Security and risk experts we consulted also noted that vendor coverage was an important point of distinction between mature- and immature third-party cyber risk management practices, especially those practices that still rely on highly manual processes for third party assessment.

Simply put: many organizations lack the tools and staff to assess the hundreds or thousands of third-party firms their employer contracts with. That forces organizations to make Faustian bargains in order to do third-party risk cyber management at all. More than one senior risk management executive described TPRM and TPCRM programs that are limited to new vendors because of staffing constraints and backlog. Their program necessarily excluded hundreds or even thousands of firms who were approved as vendors before the advent of the third-party cyber risk management program.

For many firms, simply identifying all their third parties is a monumental challenge, let alone determining their importance and their risk posture. Immature third-party cyber risk management programs are unable to scale to address the entire population of vendors and will likely address only a portion of an organization's third-party cyber risk.

Threat-focused, not Risk-focused

In addition, immature third-party cyber risk assessments may treat cyber threats discreetly: targeting the presence or absence of specific controls aimed at specific threats --desktop anti malware to combat worms and viruses, DDoS protection, strong passwords or multi factor authentication to address credential theft, etc. Alas, the whole is more than the sum of its parts, and such approaches fail to take a holistic view of cyber risk.

In contrast, mature third party cyber risk management programs focus on cyber risk above and beyond discrete threats or attack vectors. This doesn't mean third party cyber risk programs ignore the presence or absence of specific security controls. Rather, they push organizations to understand which third parties pose the greatest risk(s) and focus the organization's attention and resources on addressing those risks and that third party.

Ideally, third party cyber risk assessments reveal these vulnerabilities, first by identifying the inherent risk posed by a vendor and then by assessing the security controls used with that vendor and identifying any gaps in those critical controls. If you can surmise your level of risk absent any controls (inherent risk), it is easier to understand what controls you need in place to mitigate those risks and identify the gaps between those and your existing controls (residual risk). Taking this risk-focused, rather than threat focused approach enables you to better assess those organizations, and evaluate the assessment results.

Trusted...but not verified

Critically, legacy or immature third-party cyber risk management programs often lack the ability to verify the conclusions of risk assessments. The findings of automated scans and assessments are a great 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 comprise risk verification in the form of independent assessments, red team engagements, audits of vendor self assessments, 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 your firm.

"Companies rely more on third parties and those third parties are being given more and more data, but do not always have security program 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 vendors 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 timely and even continuous assessments of a range of security measures. 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.[15]

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.

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 un-actionable.

Your TPCRM solution should help you ~~to~~ turn risk data into concrete mitigation actions. 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.

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?

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

Prioritize your Third-Party Risks

As we noted above: even where third party cyber risk management programs exist, they often 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 firm. Informed decision making needs to start at the very beginning by conducting due diligence across 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 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 involves identifying the use case for each of your third parties, and understanding 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 this.

Understanding residual risk requires a deeper analysis of their 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(?) complicated third-party risk assessments. Often, such tools and services (think: "Slack") 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 adding them to your list of third parties that may include surveys or interviews with team leads or even individual employees within your organization to determine which shadow IT systems have been deployed.

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.

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 baseline assessment of your third-party vendors, you will struggle to accurately manage your cyber risk going forward. Key to this step is your vendor assessment: the questions you need to ask to ascertain how the vendor works with your organization.

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"[16] and ISO/IEC 127001[17] as a foundation. Many said they enlisted the services of management consulting firms with deep experience in audit and compliance.

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.

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.

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

Rank and repeat

The risk professionals we spoke with all ranked their third-party providers in some way: separating 'high risk' firms from medium and lower risk third parties. 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.

Generally, they divided vendors up into "high," "medium" and "low" risk. Middle tier firms may also 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. These vendors 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 a detailed 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

The other 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.

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.

1

Exchanges address Scale and Cost

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

2

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.

3

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 on the common exchanged 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

The most critical and overlooked step in building a mature third-party cyber risk program is to obtain the backing of your company's executives.

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 your executives and board that they will be held to account in the event (eventuality?) of a breach, 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 (n = 211) put responsibility for third-party risk at the C-suite and board level, either with the Chief Risk Officer, Chief Executive Officer or others.[18] 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.

[18] 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 of 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 continuous 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

cyber GRX

CyberGRX is a global cyber risk information exchange that enables enterprises and third parties to seamlessly share and access third-party cyber risk data. Our assessments collect data in a structured format with multiple choice questions, so users can easily run our advanced analytics for risk prioritization, continuous monitoring and to generate mitigation insights. Assessment data already in the Exchange is immediately available. Assessments that aren't in the Exchange are initiated, managed and returned by CyberGRX. Our assessments are provided in 3 tiers, covering high to low risk vendors. Each tier features a corresponding level of validation.

CyberGRX replaces static assessment processes with a dynamic illustration of third-party risk – arming customers with ongoing third-party cyber security data and the advanced analytics to turn that data into actionable insights.

the security ledger

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. We were 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 (securityledger.com), 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 LinkedIn.