CISOs INVESTIGATE:

THIRD PARTY RISK MANAGEMENT

PEER-AUTHORED RESEARCH

security current cisos connect

THANK YOU TO OUR PLATINUM SPONSOR

BLACK KITE

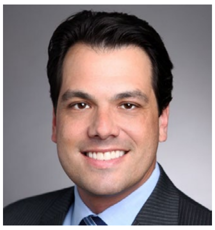
A SPECIAL THANKS TO THE CISO CONTRIBUTORS WHO MADE THIS POSSIBLE

Mike Davis
Lead Writer

Bob Turner

Patricia Titus

Colin Anderson


Matt Hollcraft

Marcos Marrero

Arun DeSouza

Joey Johnson

David Levine

Hussein Syed

Al Ghous

Marc Crudgington

Nikk Gilbert

TABLE OF CONTENTS

A NOTE FROM THE EXECUTIVE EDITOR

“We have seen better days.” - - William Shakespeare

This report began development in February 2020. As March approached, the world began hearing about a novel coronavirus known as COVID-19. As April and May withered on, we started to get used to a daily dose of remote work and saw forecasts of looming economic challenges. We began to miss Shakespeare’s better days.

Toward the end of May we were thrust into the middle of trying to understand the events surrounding the death of George Floyd at the hands of those we depend on to “protect and serve.” We are now challenged to strengthen our resolve to create the opportunity for our teams, our corporations, our countries and the world, to live a life where Black Lives Matter. Where diversity is strength.

History may not remember this report or its authors and contributors. Instead, the big news story will forever be the personal, social and economic impact of a viral pandemic that infected millions and contributed to the death of hundreds of thousands of people worldwide. We will long remember the final days of May where a national crisis that began in Minneapolis with the death of one man again highlighted our collective inattention to a serious vulnerability in our society. That we all lived with fear, uncertainty and doubt that will be the prominent historical narrative of the time.

Many of our CISO contemporaries suffered pain and loss, including some whose family members succumbed to the virus.

We all need to be committed to fighting against racism and discrimination wherever and however it exists.

We all need to search for opportunities to experience better days.

May those who experienced loss from COVID-19 or were impacted by the unrest at Summer’s onset continue to create the world we want to live in and where health and diversity thrive.

We shall never forget. We can make our world better.

Bob T

INTRODUCTION

As CISOs know, an effective TPRM strategy is not an option. Falling behind on program updates could put your business and clients at risk. With the addition of a work-from-home model for many companies, even post COVID-19, the increasing risk landscape has expanded from third party to fourth party vendors. After all, two-thirds of all data breaches can be linked either directly or indirectly to a third party.

The challenge for CISOs is fitting a TPRM program into an already busy schedule, with so many risks competing for time and attention. To make it easier to tackle TPRM, Security Current spoke with some of the nation's leading CISOs for best practices on how to develop an efficient TPRM program and integrate it into an IT and business strategy.

Consider this report as a one-stop shopping resource for all things TPRM. The CISOs' feedback provides breadth, depth, nuanced business views, multiple security leadership perspectives, and several key initiatives to tackle risks posed by third parties. Suggested steps include ways to derive efficiencies and savings (e.g., robotic process automation (RPA) efforts), increase cloud use, and others to eliminate high-profile risks like never before.

We look forward to your feedback and thoughts on this issue, and constructive discussions to come on our CISOs Connect platform and CISO-to-CISO knowledge sharing network.

About CISOs Investigate

The value of peer input cannot be overstated. Authored by leading Chief Information Security Officers, CISOs Investigate is an ongoing series that offers first-hand insights to security leaders as they make business-driven risk and technology decisions.

CISO Contributors

CISOs Investigate: Third Party Risk Management includes the viewpoints of 13 security leaders who have deployed or are looking to deploy third-party solutions. This report replaces the ad hoc, often informal and time consuming processes of personally gathering peer insight. Spanning verticals, the CISO contributors share real-world use cases and provide guidance.

Participating TPRM Providers

The report includes responses to Requests for Information (RFIs). Developed by CISOs, the RFI criteria highlight the most important technology aspects of the potential solutions. There was no cost to complete a RFI which was provided to 11 vendors identified by the CISO contributors. The following four opted to complete the RFI.

Participating Companies

BitSight
CyberGRX
JustProtect
Black Kite

LEAD WRITER:

alliantgroup
Mike Davis
Chief Information Security Officer

EXECUTIVE EDITOR:

University of Wisconsin-Madison
Bob Turner
Chief Information Security Officer

EDITORS:

Cherokee Nation Businesses
Nikk Gilbert
Chief Information Security Officer

Premise Health
Joey Johnson
Chief Information Security Officer

ServiceMax
Al Ghous
CSO and Head of Security

Woodforest National Bank
Marc Crudgington
Chief Information Security Officer,
SVP Information Security

CONTRIBUTORS:

Hellman & Friedman
Matt Hollcraft
Chief Information Security Officer

H.I.G Capital
Marcos Marrero
Chief Information Security Officer

Levi Strauss & Company
Colin Anderson
Global Chief Information Security Officer

Markel Corporation
Patricia Titus
Chief Privacy and Information
Security Officer

Nexteer Automotive
Arun DeSouza
Chief Information Security &
Privacy Officer

Ricoh USA, Inc.
David Levine
Vice President of Corporate and
Information Security, CSO

RWJBarnabas Health
Hussein Syed
Chief Information Security Officer

A CISO LOOKS AT THIRD PARTY RISK MANAGEMENT

Contributor: Mike Davis

Most CISOs understand why we are concerned about Third Party Risk Management (TPRM). Third Party's cause around 60% of all data breaches, with close to that percentage saying they share information with upwards of 100 third parties (or more). We won't go into all the downsides of a data breach or add other FUD (Fear, Uncertainty and Doubt) aspects, as you all know them just as you are all aware that they are a major risk factor for the organization. Clearly, some level of TPRM effort is essential to fulfill your 'due care' responsibilities as a responsible data steward, executing those duties in a 'due diligence' manner. This paper explores several aspects of effective TPRM execution that leadership should be aware of and which can be put into operation, especially by CISOs.

The value proposition of this paper comes from the content and views from several CISOs of different backgrounds, environments and industries. The main TPRM factors, concerns, steps and so on are presented so that leadership can decipher what matters most to them in their organization's best value approach to overall enterprise risk management (ERM) that maximizes their business success objectives. In addition, we offer a section titled "Value to the business – appealing to executive stakeholders" that provides several views with that perspective as well. That is, how to sell the TPRM program as a critical aspect of ERM to the C-Suite and board.

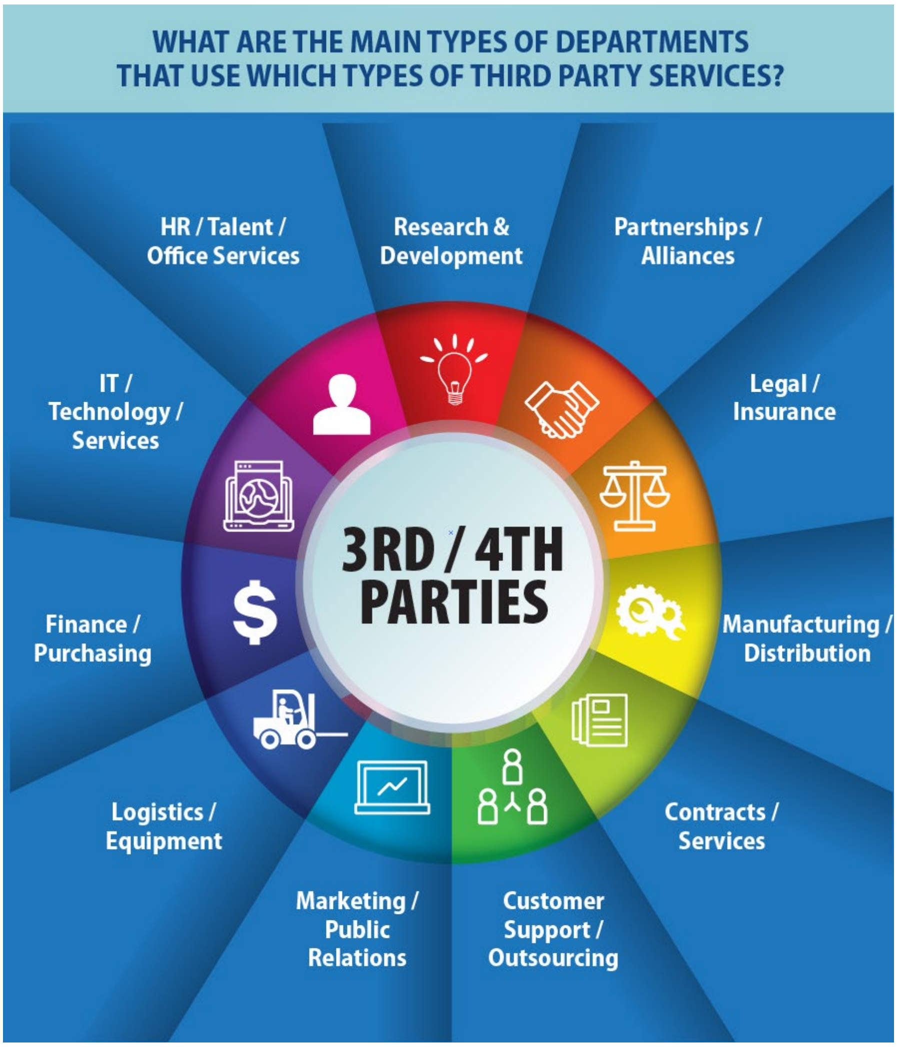
TPRM is fundamentally a supply chain analysis, using common risk factors affecting impact and likelihood. This assessment should view risk through three lenses:

- Organizational – criticality of business relationship, how much sensitive data is shared, their culture.
- Compliance – level of assurance needed, completeness of statutory requirements, any previous violations, policy maturity level.
- Technical – type of cloud usage, data processing environment, data access and storage approaches, use of subcontractors.

These lenses should be applied upfront as a pre-assessment accommodating the final, major security and risk controls and level of assurance and confidence factor required in TPRM.

Effective TPRM is not just primarily about keeping on the good side of regulators, it also reduces operating costs while helping form better relationships with customers. Thus it's an opportunity to create business value while managing risk now and into the future. To start a TPRM effort, always ask key business questions. For example:

- Why are these services being outsourced in the first place? What alternatives were assessed?
- Will the third-party potentially subcontract? Do they have data centers based overseas?
- What data is being shared? PII, IP, client data? These factors set the data security and privacy rules.
- What is the plan in case of a third-party failure or breach? Incident response plans integrated?
- What is their capability to comply with regulations? How often are they assessed?


WHAT ARE THE MAIN TYPES OF DEPARTMENTS THAT USE WHICH TYPES OF THIRD PARTY SERVICES?
3RD / 4TH PARTIES
HR / Talent / Office Services
Research & Development
Partnerships / Alliances
Legal / Insurance
Manufacturing / Distribution
Contracts / Services
Customer Support / Outsourcing
Marketing / Public Relations
Logistics / Equipment
Finance / Purchasing
IT / Technology / Services

While the TPRM high-level requirements and minimum activities may be generally understood, why is the current state so underserved? What are some of the common problems / themes that those doing TPRM now encounter?

As we all know, third party data breaches are over half the total, typically costing several million dollars; thus the need is clear, even if the execution is not (or the auditability thereof). Naturally one key question then becomes "Who owns the TPRM effort / program". In many companies, this is not consistent. While largely being led by Legal and Compliance, the lack of clear ownership hampers the allocation of resources and accountability of the process and results (or residual risks that languish). In addition, the process to get 3rd parties to mitigate discovered gaps in a timely manner (if at all) is generally not well accounted for nor actively tracked.

There are process effectiveness issues as well. The general tendency is to conduct TPRM manually using spreadsheets or simple accounting tools, whereas the use of automated and integrated tools is clearly more effective. The maturity of many TPRM programs is generally low or at best partially deployed, nor is a maturity model used to assess it therein (for example the Vendor Risk Management Maturity Model (VRMMM) by SharedAssessments.org). Also, while risk scanning and rating tools/services are used to help assess the industry data and relationships between the two parties, these are not widely used, nor are the results easily verifiable to increase the output confidence factor. As we all know, not all 3rd parties are equal of course, yet many TPRM processes do not differentiate between companies (using a process to assess the 'criticality' to the company), nor consider the 4th party connections. Finally, there are of course the litany of "execution / implementation" and management issues.

Supporting the community's understanding

While most understand the critical business need to manage TPRM, what does that entail? What types of steps are needed and in what level of detail? We offer the below overview and major points to get started (discussing some topics in more detail later):

1. **Do you have a contract management process (how do you know who to apply the TPRM to?).** Who owns it? It Seems logical that finance owns it, but do they know ALL contracts (yes, even those AWS/cloud instances that folks spin up under the radar). There are several different ways to manage post-contract relationships: auditing, monitoring, training, and ongoing communications, among them. These methods should be part of your ranking of vendors and associated contracts. By the way, this management effort goes two-ways, who does the company provide 3rd party information to?

2. **Do you have an effective TPRM policy / process?** This includes a step-by-step execution process (e.g. approve policy (and survey questions), assign critical vendors according to policy (includes business justification as needed), send survey / 'questionnaire' (tailor as needed), negotiate other assessments (this includes systems scans, Black Kite, etc), adjudicate survey findings (conduct residual risk due diligence), etc.)

3. **How do you weight /rank the relative risks – is this clear to vendors?** At what level do the various factors add up to a critical risk to remediate asap or consider contract termination (if the contract is terminated then who fills in the newly created gap)? We will address added risk items to implement later, but heads up – you will need your company's risk appetite captured, as that sets the stage to adjudicate findings, even drop a vendor.

4. **How far do you go in assessing the business relationship - 4th party, 5th?** What other relationships and connections should be included? For example, foreign companies do business differently, where 'sharing' has a lot looser meaning. This assessment should also be used as the front end of M&A efforts (adding to the financial assessments)

5. **Every question must have a risk-based response to assess and make decisions with.** For example, Business Continuity Plans (BCPs) are essential for availability of services downstream, so asking if a vendor has a plan will likely not be enough for critical vendors.

6. **Standard contract clauses for T&Cs, SLAs, MSAs, etc. will be needed to ensure the TPRM requirements** (for data security and privacy – tailored for type of contract) get formally flowed down. For example, finance/legal need to agree on the minimum areas to include: right to audit, certifications and training clauses, and the right to termination for an FCPA violation, others?)

7. **Monitoring for #2/policy** – as we know, no policy is useful unless monitored and enforced. This includes periodic reviews, mitigation follow-ups, trends / risk levels, etc. A TPRM effort needs some sort of periodic / quarterly report, including metrics. Ideally monitoring is 'continuous' or at least major changes are required to be reported shortly thereafter. One recommended overall risk approach to consider is Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA), including the TPRM aspects, which embodies "Manage Risk. Build Trust. Embrace Change by Becoming Adaptive Everywhere."

8. **Key references / authoritative sources / frameworks / standards** – these provide the requirements, methods, and guidance for your TPRM program. You need to pick a risk framework that integrates with your ERM, if not the same risk model. There are many frameworks to choose from (COBIT, ISO27001 / ISO31000, COSO, NIST, CIS CSC, etc) as well as standards to align to (HIPAA, SOX, etc), which should align to the organization's authoritative sources. Other references are provided in the appendix.

9. **Ending the relationship process: either by the end of the contract or breach in obligations:** getting formal documents, getting any data returned, etc. Contract termination releases the parties from their remaining obligations, but it does not affect liabilities for contract breaches that occurred prior to the termination, including those related to TPRM. Trying to reconstruct breach events for responsible parties after the fact are now much harder as are there is no relationship to leverage; thus forensics may become a litigation battle.

10. **Accelerating TRPM program implementation:** This type of program is heavily process based, so providing examples, templates, etc upfront is helpful both to get started and compare other artifacts and improve both. The key items to share are: TPRM policy, survey form, and contract clauses. We provide those, with links, in the appendix List of the example TPRM getting started artifacts.

OFFERING COMPETING VIEWS OR ALTERNATE THEORIES

Contributors: Mike Davis and Nikk Gilbert

While we strongly assert there is no effective alternative view of whether to do a TPRM effort or not (being fiscally irresponsible at best), there are numerous ways an attempt at a TPRM implementation can go sideways. A lack of consistent monitoring and reporting of third party risks presents major challenges for all organizations, leaving them vulnerable to downstream data breaches.

The major challenges companies face in assessing TPRM are offered next. First the obvious issue, lack of effective contract management to start with – you can't manage what you can't track and measure. Then there is frequently poor visibility into the contract or vendor ecosystem – manual systems assessments are, at best, a point in time and are updated infrequently. In addition, they can't provide an overall, enterprise, 360-degree perspective – especially something as critical as who has access and could be inside your environment. As is normally the case, a one size risk assessment process likely does not fit all vendors, where ideally you have a couple of methods that fit the industry, criticality and level of risk exposure the vendors pose. As responses are more important than the questions, some suggest the scoring be issue-based (with pre planned responses to any negative or inadequate responses). Otherwise this leads to inadequate data accuracy and quality – as survey questions vary widely – so does the TPRM team correlate, aggregate and risk rank them all?

The TPRM effectiveness and efficiency aspects are equally as diverse and interconnected. For example, the minimal utility and action based use of data provided – the vendor's view of your finding may not align with yours. How is that adjudicated and then mitigated? How would you verify the fix? Then we know the 3rd party's digital environment is a snapshot in time so the lack of continuous monitoring results in general companies using ad hoc monitoring methods that have a higher third party disruption or data breach experience. Then there is the speed and efficiency of communication between many parties, for example the relatively ineffective and slow speed of the risk assessment process. For another example, unless automated - paper surveys take a lot of time, while the environment is dynamic, changing frequently. How many survey questions have a relative risk weighting (all should), and then how are they aggregated into some overall risk value? Are these then parsed into a vendor classification based on risk levels that map back to your risk appetite and standardized responses provided? How is your overall risk mitigation plan/roadmap adjusted for these TPRM items; whereas you have your own company risk needs as well.

Cost of verification assessments (on-site, 3rd party, penetration tests, etc) are high, including more personal time to conduct. Assign the type and level of assessment according to the vendor criticality.

Then there are 'governance' concerns and aspects to address as well. As briefly mentioned, roles and responsibilities must be documented and practiced. To start with, who 'owns' the TPRM process – both sides may have an unclear reporting and ownership responsibility – thus accountability may be in question. Typically, procurement (Finance / Accounting) makes sense as they are contract centric, yet Legal and Compliance are also major actors. As are QA and Audit - are they part of your TPRM group / team? Then the contracting process and accountability measures must be clear and robust. Contractual agreements can be weak, not verifiable – as they also need to include data / privacy protection and a standard for measuring them (the appendix has a list of major items to include in contracts). Address what data is stored where and the minimum amount of data to share (as well as some indemnification should the vendor suffer a breach.) Also, which standards to invoke – being a major factor for compliance. (e.g., PCI, HIPAA, SOX, SSAE 18 SOC2, etc) and the related audit reports to request.

Process and workflow effectiveness also matter of course, including TPRM process automation to reduce unmanaged risk. Creating a standardized data capture and reporting method that can be applied to all third parties. Most organizations will need an enterprise-level tool for issue management tracking. Ideally this can be integrated with an existing GRC/IRM capability. To augment and validate self-reported questionnaires (as manual processes make using a 'trust but verify' approach difficult to implement) through independent risk-based assessments. Finally many contract management and execution processes are not mature, failing to:

- adequately assess the risk and cost of outsourcing.conduct adequate due diligence and ongoing monitoring.
- conduct an assessment before signing a contract.
- assess ALL the contract risk, for example incentivizing them to take risks in order to maximize profit.
- fully assess a potential vendor before entering into any relationship, signing a contract.

Fourth Party Risk

Every company outsources parts of its operations to multiple suppliers. Those suppliers, in turn, outsource their operations to other suppliers. This is called fourth party risk, even as that may extend to 5th parties and more. It's not uncommon for multiparty incidents to include 6-10 organizations to potentially over 100, with total damages more than 10 times that of a single party incident (Ref a.).

A fourth party vendor is someone you don't have a direct contract with but instead your vendor has a contract with them for particular products and/or services.

A couple of things you should understand about dealing with your fourth party vendors.

- Who are they?
- What products and services do they provide to your vendor?
- Has your vendor done their part of due diligence on these vendors?

Being able to better anticipate risks that may reside at a more complex level, such as how your data is shared or stored in a system that you don't have any visibility to.

A fourth party caused breach at this level can be every bit as impactful as a breach of your third party vendor. Since you don't have a direct contract with the fourth party vendors, getting access to information about what controls they have in place is next to impossible. Nobody would be interested in sharing this sort of data with a party not bound by confidentiality agreements or a need to know. It would help to talk about how you are trying to evolve and mature your vendor management program and include fourth party vendors as a concern within your risk equation.

Third Party Vendors

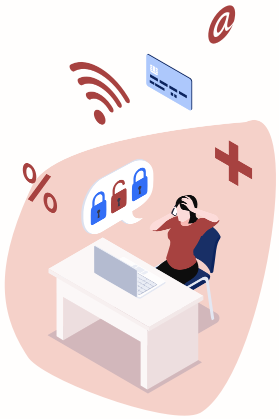
Ask your third party vendor to provide you with the following:

A copy of their downstream vendor management policy. A high risk vendor list and most recent reviews. The fourth party vendor's SOC report, your third party vendor can typically get you a copy of it, but most likely you'll need to sign the fourth party vendor's confidentiality agreement.

Once you've gathered this information, review it and formulate your thoughts of the risk these fourth party vendors pose to you. If needed, ask additional questions to ensure you understand the products or services being provided and how they can impact on your organization.

Payment processing or other dependent services for your own customers may fail if the fourth party vendor experiences a failure

Your sensitive data is being transmitted or stored by a fourth party vendor and could be exposed if the vendor's system is breached



Downtime of the fourth party vendor may be visible to your own customers depending on the integration method

Where Fourth Party Vendors Pose Risk to You

Here are a few common areas where a fourth party vendor may pose a risk to you:

- Your sensitive data is being transmitted or stored by a fourth party vendor and could be exposed if the vendor's system is breached
- Payment processing or other dependent services for your own customers may fail if the fourth party vendor experiences a failure
- Downtime of the fourth party vendor may be visible to your own customers depending on the integration method

Most importantly, document your review thoroughly and repeat annually. It's also a good idea to watch news headlines for any public information that may alert you of a breach or other potential issue with these vendors.

4th party breach story:

We had outsourced like many organizations our HSA benefits to a large 3rd party bank.

Unbeknown to us, they (the bank handling our HSA benefits) outsourced our HSA benefit accounts to a 4th party (a smaller organization which handles HSA benefits). While the fact that our HSA benefits had been outsourced to a 4th party wasn't a particular problem, although we weren't told. It seems our early contracts didn't include the right legal language for the provider to notify us if they further outsourced the benefit service.

Some of our employees had found their accounts emptied from one day to the next and so started our investigation.

RELATIONSHIPS TO POPULAR FRAMEWORKS OR INDUSTRY RESOURCES

Contributors: Marc Crudgington and Mike Davis

There are several frameworks that an organization can use when determining which framework or guideline to use. In many cases, we have found that CISO's choose to use a hybrid approach, especially those that are in a highly regulated environment where it is 'suggested' or mandated that they use a specific framework. That mindset can be due to several reasons:

- they prefer the chosen framework over the mandated framework
- the preferred framework covers some topics that are not as clear or are not in the mandated framework
- a hybrid approach ensures a more comprehensive program
- security talent is more apt to understand a multi-industry framework over a specific industry framework, etc.

We have also found using a hybrid approach that helps focus resources on areas of opportunity can be advantageous to an organization. For example, you may choose to use the NIST Cybersecurity Framework, but also add into your program Tasks from the NIST Special Publication 800-37 Revision 2 or the DoD Risk Management Framework (RMF) Revision 2 as examples.

We offer the below laws, regulations, and guidelines as a data point to help you familiarize yourself with the many available (a larger list is in the appendix). Where you reside as well as do business should play a major role in which framework(s) you choose to guide yourself. Where the data actually resides normally defines which laws apply.

Any list of the legally based references (as you can't ignore those) of what needs to be minimally addressed is essentially too numerous to provide an adequate baseline, reference for the wide audience that needs to conduct TPRM. We do offer the key privacy compliance and data security sources below, with others in the appendix; whereas the main point here is to know what applies, then take an aggregated, capstone approach to those 'must do' requirements. That is, pick the top references that directly affect your organization; then build the requirements from there adding in the significant 'deltas' as you iterate your key controls. For example in privacy, as GDPR is global and quite extensive, start with that, add in any state laws (CCPA) and those largely make up your key requirements set.

Privacy Compliance

The requirements 'flow-down' is in many cases subjective at best, and the TPRM aspects are not yet well standardized for the general commercial environment; thus we need to focus on what key laws to use, and then distill their major protections required. For many, we recommend taking the GDPR privacy requirements as a worst case (yes you need to assume this DOES apply!), then adding in the CCPA and FTC unique mandates, followed by your state laws. This baselines your requirements. For many the privacy requirements in HIPAA, GLBA, and others will also apply.

- **GDPR** --- The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though passed by the European Union (EU), it imposes privacy obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. (Ref d.)

- **CCPA** --- Second only (so far) to the GDPR in scope, the California Consumer Privacy Act (CCPA), covers for-profit entities if California based consumers personal data is collected, shared, or sold, and:
  - ⇨ Has annual gross revenues in excess of $25 million; or
  - ⇨ Possesses the personal information of 100,000 or more consumers, households, or devices; or
  - ⇨ Earns more than half of its annual revenue from selling consumers' personal information.

So, do you think you don't fit the first requirement? Okay, can you explicitly prove the negative – that you never collect data on any Californian? Likely not, there are many input vectors. (Ref b.)

- **FTC** --- their legal authority is from the Federal Trade Commission Act, Section Five, which prohibits unfair or deceptive practices in the marketplace. Their main tool is enforcement actions to stop violations and require affirmative steps to remediate the unlawful behavior. They are the USA's privacy watchdog and their enforcement activities have been growing, as well as their fines. (Ref c.) If you have a privacy officer, lead or equivalent manager of any sort (as we're not assuming you need a "DPO" for this paper), it's best to capture the key privacy controls the organization needs assessed, then embed them in the survey, we recommend capturing them in a separate privacy section. Again, these questions need to be risk based and the response then parsed to pre-assessed levels of compliance. For example, some privacy related potential questions could be:

  - ⇨ Is personally identifiable information (PII) being collected or processed? If so, please document which types of PII are used, by whom.
  - ⇨ Does the entity collect PII on people in the EU (GDPR) or CA (CCPA), thus those privacy laws are applicable.
  - ⇨ Where are all the potential data subjects (i.e. the individual to whom the PII relates) located. For example:US, worldwide, EU.
  - ⇨ Are there data protection policies and processes in place? If so, please provide details.
  - ⇨ Is there a dedicated data protection "manager"? If so, who? If not who assumes those roles?
  - ⇨ Are employees trained in data protection compliance? If so, please provide details.
  - ⇨ Is there a process for recording and responding to suspected/ actual data breaches? If so, please provide details.
  - ⇨ Are there data retention and deletion policies and processes in place?

Data Security Risk

While data security is a little more quantifiable in the flow-down aspects than privacy, it covers a lot more security controls; thus which reference should take precedence, lead your requirements, set your security risk foundation is a critical choice. In general for the USA we propose that CIS CSC + NIST is an effective reference set; whereas globally the ISO set is likely more germane. For those focused on accounting and the financial sector COBIT + COSO may be the best.

- **ISO/IEC 27001(infosec) / 31000 (risk) / 27701 (privacy) -** The globally accepted 'gold standard' of security and risk references. Generally provides much more in depth controls and specificity; whereas that also takes a lot more resources to assess and then mitigate. These controls may not 'flow-down' to many 3rd party entities.

- **COSO and SSAE18 SOC1/2 -** The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an approach to Internal Control Framework. The COSO Framework was designed to help businesses establish, assess and enhance their internal controls, with five components and 17 principles. (Ref e.)

- **+ SSAE18 controls** are a series of enhancements to increase the usefulness and quality of SOC reports, superseding SSAE 16, and, the legacy audit report, SAS 70. (Refs f. and g.)

- **NIST Cybersecurity Framework -** National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was published in response to Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which called for a standardized security framework for critical infrastructure in the United States. It is composed of five elements and 108 security controls. It is in wide use by around half of all commercial entities. (Ref h.)

- **CIS CSC -** Center for Internet Security (CIS) Critical Security Controls (CSC) (V7.1) provides guidance to prioritize controls utilization, known as CIS Implementation Groups (IGs). The IGs are a way to help organizations classify themselves and focus their security resources and expertise. (note - frequently called the 'top 20 security controls') (Ref i.)

- **CMMC –** For the federal / DoD types, there is obviously the recent, federally mandated Cybersecurity Maturity Model Certification (CMMC). It builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity. As it's required to bid on federal contracts, so if you have one, then you have to do it. (Ref j.)

The data security risk framework choice can be problematic as in the high volume of controls to assess as part of the survey, questionnaire based risk assessment. Add to that the fact that all 50 states have some level of data breach reporting requirements and this area alone becomes a TPRM resources driver. Thus using a known, authoritative source's questionnaire is the best approach – standardization is crucial, as you will have many vendors' responses to capture and you have to risk rank and then track them all too. Also, you'd need to include mitigations. (see Ref k.)

In short, take a global privacy compliance approach in your TPRM; then tailor / thin it down as needed.

For those wanting to use NIST and other related auditing resources, see:

https://www.nist.gov/cyberframework/assessment-auditing-resources

Where Data is Gold

In a new world where data is the new gold, privacy risks are increasing at a rate that is challenging to keep up with. Hence, the recent explosion of new privacy laws that attempt to reel in the risks of privacy or penalize those that do not adhere to them. Though we believe it is important to remember and we have found when dealing with cybersecurity risks that often you can be compliant, but not secure; it is rare that when you can say you are secure that you will not also be compliant. Point being that following a framework, regulation, law, and so on is not the end all be all.

Reasonable Security

What you consider reasonable security is dependent on the risks your organization faces as well as the laws organizations in your industry and/or the states you operate mandate that you follow. Though many organizations are similar (size, risks, operations), no one organization is the same. Choose a framework(s) to follow that fits your organization and follow a maturity model that will allow you to measure and appreciate progression as your program matures.

You will likely need to state what your expectations are for 'reasonable security' - as that applies to your environment as well. Most laws and regulations describe this security posture state as vague as possible. You will need to define it clearly to be understandable by all third parties. Your requirement should be reflected in their data and privacy protection methods they plan to implement. In short, there is only one published 'legal' artifact that calls out somewhat definitively what 'reasonable security' entails. That is the FEB 16, 2016 CA AG report " California Data Breach Report 2012-2015" which essentially states using the CIS CSC risk framework to measure your status, risk levels[1].

Considerations for Environmental Components or Issues

How does one grapple with the vast number of risk vectors to account for (e.g., IoT, wearables, 5G, mobile first, etc). What other environmental aspects and types of risks can there be from an inadequate TPRM effort, such as:

- Reputation when 3rd/4th party comes under legal scrutiny or has negative publicity (breach / privacy violation, etc)
- Strategic investment ineffectiveness from an inadequate risk assessment's residual risks and not knowing about a new product, business line, or activity.
- Compliance when not fully aligning with laws/statutes or the company's policies and procedures, or audit and controls are inadequate
- Performance from the failure to deliver services for any reason, not meet the contract terms.

Clearly the ability to effectively conduct a risk assessment and then decide on the risk acceptance decision process is critical to the overall program. Many indicators show that this phase of the effort is not well documented, or applied consistently, or in fact applied at all in some cases. The Questionnaire must itself be risk based and all responses be weighted. Then we suggest using a risk triage approach – putting 3rd parties into tiers – inherent risk factors they have, and overall weighting / scoring model based on those levels needed to meet the organization's inherited risk appetite (the required enhancements of security and privacy controls). Yet to make that risk decision, the organization needs to understand the residual risk a third party presents in relation to its capacity (and ability to be swapped out if needed) and criticality in your supply chain and quantify the risk appetite as well as risk tolerances and thresholds therein.

The risk assessment needs to target specific success factors to the business relationship. That means the risk equation must include: appetite, capacity, tolerance, targets, and minimally acceptable risk levels.

[1] *For more details see the article (Ref I.)*

ONE CISO BUILDS A USE CASE

Contributor: Bob Turner

As stated earlier, partnering with other businesses means the opportunity for profits and innovation need to be considered in relation to activities of the partnership that place your corporate data at risk. Large organizations which offer services in addition to consuming them need to look at TPRM from at least two perspectives, risk taker and potential risk maker. These competing parts of the risk management business should consider risk as a set of complimentary activities, where one control offsets another, there should be a clear set of definitions and vetted examples to show the corporate leaders. The TPRM program must include as major components vendor acquisition and onboarding, assessment and rating of risk, credential and certificate management, plus reporting and analytics. These risk components need to be viewed in context with shared information technology, data management, service provider risk, and relationships with channel partners.

Consider the issues when your third party has a data breach or a major malicious code infection:

- Was your data involved in their breach?
- What was the nature of the trust relationship between your IT systems and theirs?
- Are corporate risk appetite's congruent, or is one business more strict or more relaxed?
- How does your third party prioritize risk assessment, reporting and remediation?
- What part of the technical architecture was analyzed for risk from both partner's perspectives (i.e., encryption, access management, data governance, etc)?
- How often and how are you examining each partner's risk posture and is that set of assessments considered in your own risk management structure?
- Did they make the right reports to outside parties or government agencies (e.g., GDPR, CCPA, HIPAA FERPA, etc)?
- What was their 6 o'clock news story headline and do they coordinate before press time?

Other areas to explore include the life cycle of third party risk, data sharing, risk tolerance, customers that are jointly held between the two corporate entities, and resiliency in the face of the constant levels of stories in the news cycle.

The TPRM Process

There are many approaches to the workflow and major steps in TPRM. Similar to the popular cybersecurity frameworks like MITRE ATT&CK or the NIST Cybersecurity Framework, TPRM has specific activities that are important to a well run program.

These steps may include:

Planning - In this step the business determines what the need, scope, and specific outcomes should be. Determining the type of assessment desired (e.g., phone interview, questionnaire, self assessment) would happen in this step.

Conducting a Kick-off Meeting - Agreement on the scope and outcomes along with the desired activities would be outcomes of this important meeting. Determining key legal issues like use of data, retention, records required by law or industry standards, key players, and establishment of authorities are all activities worth considering.

Starting the Vendor Engagement - This is a formal activity that sets the pace - it may be combined with other activities and is important to be conducted with all players present. A thorough review of procedures at the start of the engagement will make the assessment successful.

Data Exchange - Key to communications are detailing the types of data that may be exchanged, including security considerations for proprietary information, trade secrets, and other sensitive or restricted information. Consider where and how data might be shared, stored, analyzed, and be sure to document the requirements for data security following the assessment.

Analyze and Document Findings - This stage is the responsibility of the business unit assessing a vendor. Processes may vary, but the outcome is the responsibility of the responsible assessors and their management.

Communicate Results - Follow standards for your particular industry and communicate early and often during the assessment. Remember you are trying to justify the relationship continuing to the next stage.

Remediation Planning and Follow up - No assessment is perfect. Ensure both parties agree on remediation activities, plan the steps, and hold to the timelines.

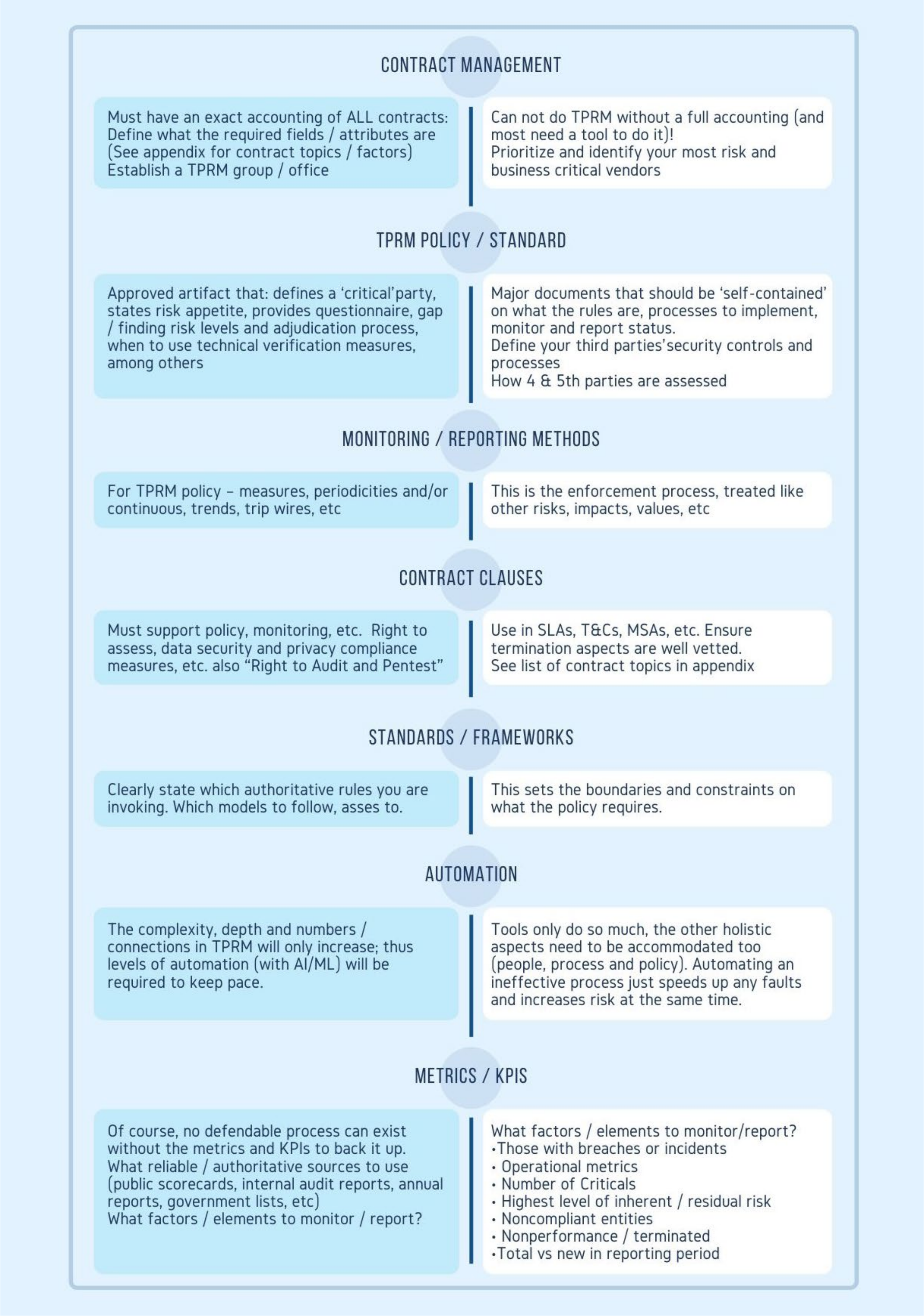
RECOMMENDATIONS TO PEERS

Contributor: Mike Davis

Given the above rationale, guidance, major concerns, and recommendations, what must an organization do, what are the high value / priority activities? To recap and restate those aspects, we propose a generalized list of TPRM program activities. As always, we need to get the requirements right first, in this case - understand your compliance landscape – assess and capture relevant laws, statues, & regulations. Then since risk is our lens, quantify key risks within the TPRM program – align the risk appetite for each. Integrate TPRM execution approaches/ processes (including monitoring,findings adjudication, incident responses, etc) into the existing organization business processes, as they cannot be siloed as the process based risks can become significant. Along with a risk based process focus, is the need to capture company objectives for due diligence levels of residual risk.

Even more process related efforts must be integrated to minimize the gaps and maximize effectiveness. For example, define contract key attributes, thresholds to assess both data security and privacy clauses – develop a TPRM survey (questions and methods), strive for a low overhead, high risk assessment value. Ensure a robust contract management process is in play, fully vetted attributes to capture and report, assess and assign critical characteristics, screen for sanctions, watch lists and PEPs (politically exposed persons). Then develop KPIs / metrics to maintain trends, residual risk status, provide monthly reports, etc. consider a 3rd party risk catalogue to share with senior leadership, key stakeholders. Follow that by piloting the process with a few critical companies that have existing good relationships – conduct the risk assessment / validate the information collected, share lessons learned. Then there is the audit aspect - the due-diligence process itself – set up a self-assessment method and periodicity. Supporting this by establishing an on-going monitoring plan – include periodic incident exercises that include 3rd parties. Finally, the all-important periodic reports to leadership, sharing with 3rd parties, major stakeholders.

The following table provides additional details for the overall TPRM tasks/steps list – how to get started:



CONTRACT MANAGEMENT

Must have an exact accounting of ALL contracts:
Define what the required fields / attributes are
(See appendix for contract topics / factors)
Establish a TPRM group / office

Can not do TPRM without a full accounting (and most need a tool to do it)!
Prioritize and identify your most risk and business critical vendors

TPRM POLICY / STANDARD

Approved artifact that: defines a 'critical'party, states risk appetite, provides questionnaire, gap / finding risk levels and adjudication process, when to use technical verification measures, among others

Major documents that should be 'self-contained' on what the rules are, processes to implement, monitor and report status.
Define your third parties'security controls and processes
How 4 & 5th parties are assessed

MONITORING / REPORTING METHODS

For TPRM policy - measures, periodicities and/or continuous, trends, trip wires, etc

This is the enforcement process, treated like other risks, impacts, values, etc

CONTRACT CLAUSES

Must support policy, monitoring, etc. Right to assess, data security and privacy compliance measures, etc. also "Right to Audit and Pentest"

Use in SLAs, T&Cs, MSAs, etc. Ensure termination aspects are well vetted.
See list of contract topics in appendix

STANDARDS / FRAMEWORKS

Clearly state which authoritative rules you are invoking. Which models to follow, asses to.

This sets the boundaries and constraints on what the policy requires.

AUTOMATION

The complexity, depth and numbers / connections in TPRM will only increase; thus levels of automation (with AI/ML) will be required to keep pace.

Tools only do so much, the other holistic aspects need to be accommodated too (people, process and policy). Automating an ineffective process just speeds up any faults and increases risk at the same time.

METRICS / KPIS

Of course, no defendable process can exist without the metrics and KPIs to back it up.
What reliable / authoritative sources to use (public scorecards, internal audit reports, annual reports, government lists, etc)
What factors / elements to monitor / report?

What factors / elements to monitor/report?
- Those with breaches or incidents
- Operational metrics
- Number of Criticals
- Highest level of inherent / residual risk
- Noncompliant entities
- Nonperformance / terminated
- Total vs new in reporting period

TO SUM IT ALL UP…

Contributor: Bob Turner

The bottom line is not whether to have a TPRM effort or not, but rather how extensive it is, or needs to be, to prove in a court of law that an adequate due diligence risk assessment was accomplished and the communications between all parties was equally effective.

A Use Case for implementing TPRM

One use case in a Midwest company involves that company acting as a 3rd party to multiple other corporate entities. This company also engages third party entities to perform work such as cloud storage and architectures (SaaS, PaaS, or IaaS).

Being responsible for other's data must be treated at the same level of the expectations this company has of their vendors and service providers. This company, which we will call Company A for this section, engages with their vendors and service providers early enough to negotiate a common approach, taxonomy, and metrics structure so risk is leveled between all parties. Using the 2017 report from U.S. Chamber of Commerce titled "Principles for Fair and Accurate Security Ratings" the parties settle on a set of principles that define:

- how transparent they will be with the data and systems where the data lives;
- processes for handling disputes, corrections or appeals;
- governance models for ensuring data privacy and confidentiality;
- frequency and depth for periodic audits; and
- how to maintain independence of the teams assessing risk in each environment and across the digital borders. (Ref n.)

Company A also ensures the definition of risk is understood and agreed on to drive the common risk equation. Normally, the chosen risk statement is congruent with the FAIR Institute's definition of risk which states "risk is the probable frequency and magnitude of loss." (Ref o.) Defining risk severity using the Common Vulnerability Scoring System (CVSS) (Ref p.) and a level understanding of the asset value. Asset value in this case includes the property value of the data which may include personal identities, medical information, financial or tax records, or the cost to recover corporate records such as e-mail, formal reports, or other records, and the cost in hardware, labor and licensing to recover platforms or infrastructure.

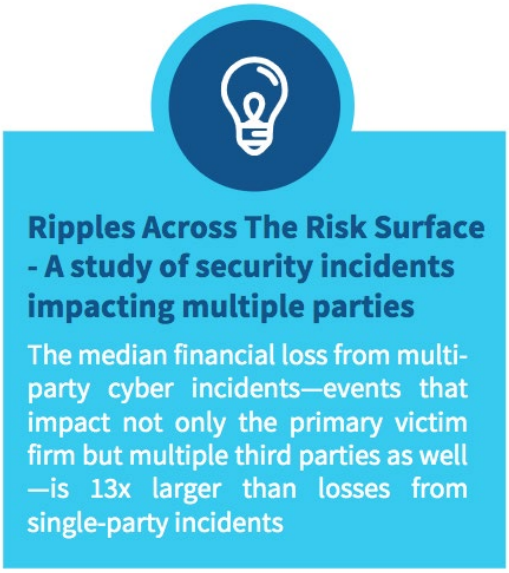
After deciding these key issues, there is a transfer of the information or resources regulated by contract, and work begins. Both parties self-assess risk periodically throughout the engagement, reporting when risk changes up or down. As the engagement ends, the return of information assets and resources is conducted, or disposal is ordered by the party owning the resource. All projects result in a report which may take the form of a published research paper which then becomes Company A's owned intellectual property. The next section offers several other views and considerations.

TECHNOLOGY OVERVIEW: KEY CONSIDERATIONS

Core Features of Recommended Solutions

Contributors: Al Ghous, Bob Turner, Mike Davis, Marc Crudgington

We propose that TPRM is mostly a policy / process driven function… supplemented by some products to help track and report (especially those large companies). Since we strongly suggest that it is irresponsible (at best) to NOT have some minimal level of TPRM effort, our proposed counter argument revolves around not going beyond just the 'mechanical' TPRM activities – and the added risk to the organization those miscalculations affect.



Ripples Across The Risk Surface - A study of security incidents impacting multiple parties

The median financial loss from multi-party cyber incidents—events that impact not only the primary victim firm but multiple third parties as well —is 13x larger than losses from single-party incidents

For more details see the article (Ref r.)

There are more than a few areas that a CISO should consider when starting, evaluating or maturing your organization's Third-Party Risk Management program. As with many things related to cyber/risk, your considerations are dependent on the industry, risks, complexity, and culture of your organization. Listed here are some considerations and a little about each.

1. **Executive Sponsorship is key to a successful TPRM program** - The Board and C-Suite are accountable for risks at your organization which includes third-party risks. The Board and executive management should want to know what risks third parties pose to the organization so they can account for it and direct appropriate actions. This is a two-way communication pipeline between the Board and executive management and those charged with managing the TPRM program.

2. **Assess Current Status of your Program** - One of the first steps to moving is knowing where you are at. This may be as simple as acknowledging you don't have a program in place, or it could be measuring the gaps in your current program. If there is a program in place, think of the potential to hire an outside firm to assess your program if budget allows. Otherwise, an objective assessment can provide what is necessary.

3. **Use a Collaborative Approach, not Siloed** - A TPRM program should leverage staff from many areas of the organization from Legal, IT, Security, Finance, Procurement, and others. Incorporate information pertaining to the Program in Executive Meetings such as third parties added, third party incidents and risks, details about the program, etc. The Program managers should commit to communicating information about the Program to Stakeholders on a frequency that makes sense for your organization's complexity and the Program's maturity

4. **Implement Repeatable, Mature Processes** - Repeatable processes should be standardized across all departments and functions within the organization. A policy should govern the Program with processes documented and well defined; training should be readily available to either deliver via your Learning Management System or through knowledge base artifacts. Not one person in your organization that has gone through the process shouldn't be able to describe the process or point to where the information can be found.

5. **Due Diligence should be based on the Third-Party's Risk Profile** - Organizations that are more mature in their Third-Party Risk Management program use an approach based on the inherent risks that the third party presents as not all third parties are equal in risks. Many organizations tier assessments into levels based on the risk profile. A simple structure would be Low, Medium, High or Level I, II, III or something like that. The screening and due diligence would be dependent on risks and data provided to or access granted to the third-party organization. The initial assessment is the foundation of a strong, effective, and mature Program. Additionally, assessments should be frequent after the relationship has been established with continuous monitoring through real-time alerts/news feeds or a technology solution.

6. **Fourth Parties should also be assessed** - When assessing a third-party, fourth parties – organizations that the third party uses or may use for services – should also be inquired about. You may be using a third-party SaaS provider, but you will also want to assess at some level where their application is being hosted. This could have ramifications for several data privacy laws depending on the countries you are operating in. Don't forget the Fourth Parties.

7. **Focus on the Third-Party's Technology Risks** - Chances are that if you have trouble with a third-party, it is the technology aspects that will be the root cause. It could be too much access given, outages that cause downtime to your services, ineffective security practices that cause a breach, etc. Your customers or your organization isn't going to care about the third or fourth party, they will hold your organization accountable. To reiterate above, your focus should be based on the inherent risks the third party presents. A landscaping vendor is not going to pose the same risks as your hosted Human Capital Management system.

8. **Utilize Technology where feasible** - Technology in the third-party ecosystem can integrate into many areas. We mentioned above about news feeds and alerts when monitoring them. Think about a vendor management system that manages all third-party vendors that includes workflows for the initial assessments and periodic assessments that also serves as the document repository system for all vendors. How about a rating system that may describe risks whether operational or financial a vendor may pose? Using technology can streamline the process and make your program run more efficiently.

9. **Adequate Investment in Staffing and the Program** - You will no doubt have to invest in your TPRM Program with either time, resources and/or technology. The investment is up to you and how robust of a program you want to create and maintain. The risks third parties pose is not one to be ignored, they can put your organization out of business if not addressed. At a minimum, your organization should assign someone as the Program Manager and an Executive Sponsor. Whether the Program Manager is hired or assigned from current staff would depend on complexity and risks. Standing up and/or measuring the effectiveness, then subsequent monitoring should be treated with the same diligence as any other major program in your organization.

10. **Measure the Effectiveness** - Like the famous New York Yankee Yogi Berra once said:"You've got to be very careful if you don't know where you are going, because you might not get there." That quote rings very true with a TPRM program, it must be measured and monitored to know its effectiveness. This can be done internally or by an external firm. Good points to measure would be after you have defined the program

PRODUCT OR SERVICE	DESCRIPTION
THIRD PARTY ONBOARDING	Product should establish an enterprise-wide process to introduce potential providers. It must be implemented in a manner that leaves no racks for the business to engage a partner without proper due diligence.
THIRD PARTY DUE DILIGENCE	Product should establish objectivity in the pre-contract assessment process by facilitating building and sending context-based questionnaires to vendors as well as processing the answers and automatically assessing objectively against the organization's policies.
ONSITE CONTROLS ASSESSMENT	Those third parties that serve mission-critical functions, or have access to sensitive data, your organization may need to schedule on-site visits to make visual verification of compliance and contract conformance.
THIRD PARTY PERFORMANCE REVIEWS	Ability to not just initially assess but ensure that partners are continuously meeting their obligations via automated workflows and scheduled reassessments. Goal is to complete re-assessments faster with more consistent results.
THIRD PARTY CONTRACT MANAGEMENT	Ability to store and version control third party MSAs, DPAs, certifications, reports, and other artifacts for easy access.
THIRD PARTY SLA MONITORING	Ability to monitor third party commitments in terms of SLAs, RPO and RTO times.
THIRD PARTY RISK RESOLUTION MANAGEMENT	Ability to identify and track third party issues and risks provide workflow to facilitate timely resolution.
SECURITY AND PRIVACY COMPLIANCE SCANNING	Ability to identify key third-party vendor changes that could impact privacy, security, or compliance.
ROBUST REPORTING	Create reports, monitor risk mitigation over time, and identify the organization's riskiest third-party vendors.
GLOBAL SCOPE	Ability to meet the organization's security and privacy compliance challenges with a third-party that spans industry, jurisdiction, and region.
RESEARCH AND DEVELOPMENT	Provide the ability to get ahead of regulatory changes before they occur at global scale by providing industry research and guidance.

– will this be an effective TPRM program – then approximately 6 months to 1 year after it has been implemented and periodically after that. Areas of the program to review could include policy and processes, controls for the program, surveys to stakeholders, efficiencies when onboarding vendors, effectiveness of identifying vendor risks, appropriate budgeting and staffing, and several other points. The objective is to determine if the Program requires any improvements and how well it is running.

There is no shortage of platforms or point solutions that can help organizations manage their third-party risk. One can go back to the initial days of Governance, Risk and Compliance (GRC) products where vendors began to realize how important third-party risk was going to become. As these GRC vendors started to add Vendor Risk modules to their products, it was natural for CISOs to leverage one platform for their governance, risk and compliance efforts.

Since the introduction of vendor risk management capabilities within GRC platforms, there have been a plethora of products that offer modules specific to managing vendor risk. For the most part they have been rich in features and capabilities. However, over time we have found that they have become heavy and confusing to use, which have caused customer frustrations. Furthermore, the approaches of assessing third parties have also evolved over time. Aside from the traditional approaches of sending out questionnaires, evaluating risks and managing a workflow, another breed of solutions came to market that use data-driven, dynamic measurement of a third party's general security performance that enables more efficient and effective assessment of risk via a final score.

For CISOs who already have a Third Party Risk Management (TPRM) product but seek validation that they have selected the right partner, or for those that are thinking about purchasing one to support their respective programs, the below criteria should help identify the product that best meets your criteria. Please keep in mind these features and capabilities are not meant to be exhaustive, but it will help CISOs focus in the right direction.

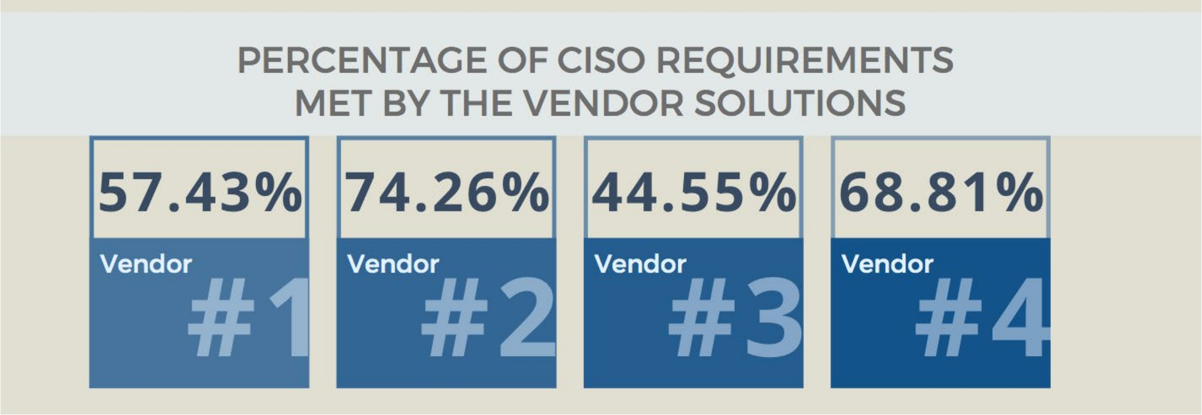
What does the vendor community provide?

A small team of CISOs evaluated the RFI responses (shown in Appendix A – RFIs). All solutions offer automation and data visibility which provides great insight on the supply chain vendor approaches to security and risk. Though all of the TPRM vendors differ on analytical approaches, two of the four respondents stated they use a specific framework.

Vendors also varied in the depth of describing how their company's product or service met the CISOs requirements. Though some just answered with a "yes," others went into great depth. All solutions share data with the third party vendor being assessed which is great for transparency, though it may cause the party assessing risk to have more restrictive data management chores if an assessment responses are retained.

More detailed information is shown in the Market Assessment section of this report (starting on page 46).

In order to help CISOs get started with their RFI/RFP process, a sample RFI/RFP template is being provided to help the process move forward. CISOs and their teams are encouraged to review and modify the template as they see fit given what is important to them from a TPRM perspective.



SELLING TO THE C-SUITE

Value to the business – appealing to executive stakeholders

Contributors: Joey Johnson, Mike Davis, and Marc Crudgington

A TPRM program delivers significant value to the business above and beyond just dealing with vendors and reducing inherent risk therein. These concepts get the appropriate visibility at the leadership level to truly pull them in as committed and engaged stakeholders. Some of these are concepts, but they hold up to significant scrutiny from most major clients who audit extensively and the maturity of a TPRM program.

Launching and managing a successful TPRM program can provide risk reduction to the organization in ways that are both obvious and significant. But truly garnering executive and board level stakeholder support often requires highlighting some of the not-so-obvious, but equally material, TPRM benefits the organization. The key is that a TRPM function is not just 'another security risk management' effort. It's value to the organization is inter-departmental and will be realized in phases, where business value is continuously delivered ahead of the cost and resourcing required to drive the program.

It is important to highlight these outcomes in early stage discussion with leadership stakeholders. Garnering support from this audience comes much easier when they can understand the program roadmap and the value that it delivers as it matures. Aside from its primary stated objective of tangible security risk reduction, which much of this paper focuses on, a mature program will serve to provide significant cross departmental business alignment between the overall Security Program and the myriad of business initiatives. In fact, a well implemented program can be so transformative that it dramatically changes the way the broader business perceives and engages with the security function.

DISCOVERY PHASE: Driver of Business Efficiency

A successful program will start with discovery of the vendor universe inside the organization today. This discovery process alone will drive collaboration between key stakeholders across Security, Legal, Procurement, Finance, Operations, etc. While the initial discovery process is a heavy-lift it can generally be completed without a significant financial outlay. However the results of the discovery, if presented properly, will provide some immediate BUSINESS level benefits such as:

Identification of redundant and/or duplicative vendors

Simply reducing this pool provides immediate benefits to Procurement, Legal, Accounts Payable, and Operations departments. There are less vendors to legally paper, manage, pay. Focus can be put on the fewer remaining vendors for procurement pricing leverage as well establishment of better direct partnership-oriented relationships with this smaller vendor population. This provides immediate measurable business level direct and indirect cost efficiencies from the TPRM program. A case can be made to redirect a portion of these savings to further fund the program.

Tool to Drive Enterprise Standardization

The resulting vendor discovery also provides opportunities to meet with various key stakeholders and identify opportunities for standardization within their vertical. A real-world example in a healthcare provider environment would be the identification of multiple different radiology vendors and products in use. When presented to clinical leadership the outcome was that security concerns aside, many of them did not align with current clinical leadership perspectives of clinical best practice or approaches by the organization. The TPRM discovery process alone provided visibility to this problem and allowed the clinical leadership team to manage reduction of the associated vendor population based solely on clinical drivers. It empowered them to create standardization criteria for radiology product and vendor selection. This in turn reduced the breadth of the vendor landscape thereby immediately reducing overall risk to the business. Furthermore, the Finance department voiced concerns regarding hardware deprecation requirements, which drove certain legacy components (and their associated vendor support personnel & platforms) out of the organization, thereby further reducing third-party footprint. This process can be repeated across departments to identify where 'rogue vendors' have emerged over time and provide a way for departments to correct those actions and put in place governance guardrails to prevent this on a go-forward basis. This delivers tangible risk reduction value by reducing the vendor pool before a single assessment has been sent out.

Tool to Drive Interdepartmental Alignment

Initial vendor discovery, if done properly, will generally identify organizational governance gaps in vendor selection. Oftentimes Procurement departments have not been provided appropriate selection gating criteria upon which to reject requests. A particular purchase request may meet the requesting department's needs, but not meet the baseline requirements of IT, Compliance, Finance, etc. A properly launched TPRM will provide an inter-departmental communications platform whereby all the necessary stakeholders can ensure alignment that a new initiative or vendor SHOULD even go-forward before it makes a Procurement to pursue. With that direction a successful program will provide a 'procurement safety net' triad between Security, Legal, and Procurement, with these three departments serving as the collaborative gating mechanism by which new things enter the organization. A key element to this success is the creation and implementation of a Third Party Security Requirements (TPSR) document which accompanies all relevant contracts and defines the terms a third-party must meet.

Note that much of this very tangible business value from the TPRM program is realized before its primary business function of security risk reduction has even commenced! Presented in this context the creation and early RoI of the TPRM program provide compelling use cases for garnering executive support. The very existence of the program drives scalability for the organization and highlights fundamental operational and communication gaps within the organization. The discovery process alone creates program visibility and develops business relationships with the Security/GRC TPRM function that will serve to keep the program tightly aligned with broader business objectives. This also provided the broader Security/GRC function visibility into critical business context and priority that will help them to shape risk tolerance decisions.

BUSINESS OPERATIONS REMEDIATION PHASE: Closing Gaps

Identification of 'Non-Vendor' Third Parties

If the discovery phase is scoped appropriately it will look beyond 'known & contracted' vendors and additionally aim to identify where data exports are occurring within the organization. There are numerous high-risk data transfer scenarios to external parties who are not formally contracted in any capacity, nor are they being paid in any capacity. However, the data moving to those third parties may represent significant risk and direct liability to the business. While these parties are generally known entities to the specific department that interacts with them such as IT, Client Reporting, etc; they are typically unknown to key compliance and financial governance stakeholder functions in the business such as Legal, Compliance, Privacy, Accounts Payable, Procurement, etc. Due to this there are likely no risk management controls in place with these parties. Articles like Data Exchange Agreements need to be drafted and put in place, and the TPRM program will need to maintain visibility of these parties.

Implications on Cyber Insurance Coverage and Business Continuity Strategy

Holistic identification of the organization's vendor landscape has direct ramifications on the organization's business continuity strategy. An effectively communicating TPRM program will highlight business workflow dependencies that may not have been fully visible outside the singular business function that is leveraging them. The TPRM program should work closely with the Enterprise Risk Management and Business Continuity Programs to ensure that as the third-party landscape evolves and changes those risk levels are mapped into the overall business risk tolerance awareness.

Similarly, most modern cyber insurance programs inquire about the third-parties the organization is reliant upon when scoping coverage and pricing premiums. Ensuring that the appropriate third-parties are identified and called out to the stakeholders negotiating the policy is critical to protecting the organization.

Drive & Highlight Risk Acceptance Accountability

An additional value of the initial TPRM discovery process is that it identifies not only the third-parties in use, but also who is procuring and using those services. It is not uncommon that those individuals have made their selections without considering or fully understanding the risks that may introduce to the business, of which security is just one flavor. An effectively communicating TPRM program will highlight to high-level business stakeholders that while senior management may have a certain set of expectations around risk tolerance (which may even be codified in policy) the actions of numerous groups or individuals within the organization are operating at a level above that risk tolerance threshold. Providing visibility to this issue should facilitate a change in organizational governance structures. It should also highlight that where business decisions are made regarding a third-party that knowingly exceeds defined risk acceptance levels, that there is an accountability for those actions. Executive stakeholders understand the various flavors of risk inherently – Financial risk, execution risk, perception risk, etc. As mentioned, security risk is just one more flavor. Executive stakeholders are constantly evaluating where and how to take risks, and even leverage those decisions as a competitive advantage. But where there is a gap between that executive perception of tolerable risk acceptance, and risks that the business is actually accepting in its operating practices, those senior level stakeholders want to know about that. A TPRM program is a powerful mechanism to provide them that insight, while simultaneously continually increasing the degree to which the program itself becomes a critical and indispensable core function of the business.

VENDOR REMEDIATION PHASE: Directly Reducing Vendor Risk

Bring Existing Partners into Compliance

Implementing a third-party risk management program with new vendor partners represents a heavy-lift to get all the governing documentation together, ensure internal departmental stakeholder alignment, and then navigate through legalese negotiation and redlining. But collectively those steps do serve as a very early stage risk assessment of a vendor by identifying key areas in your security documents that they can't or won't agree to (Beware the vendor who blindly accepts any requirements you send over without further discussion!). It sets the foundation at the beginning of the relationship for what the risk level is, and expectations around how that will be managed.

Managing Internal Stakeholders

However, existing partnerships present a very different and often more complicated set of challenges. These may be partnerships that are years old, and the notion of suddenly introducing rigorous new requirements into the partnership is an endeavor that needs to be navigated carefully. For new vendor partners all context is set up front as the relationship is formed, and it is formed wholly cognizant of both the reality and criticality of security requirements. But existing partnerships were frequently formed in the absence of these requirements. Admittedly, the demands of meeting these new requirements would be fairly unattainable to existing partnerships. They were implemented based on personal relationships, very specific levels of subject matter expertise, and/or the flexibility that their small business nature presented.

The very same qualities that made them a preferred vendor and highly integrated partner, now represent the same qualities that make them an undesirable partner based on security risk. Internal stakeholders closest to these relationships will naturally feel threatened by the notion of deconstructing what has historically been a very strong partnership, often with personal relationship ties. So addressing this requires navigating complicated scenarios that extend beyond a security findings report. Something critical to be aware of as you embark on your path. At the end of the day the requirements are the requirements, and don't need to waver. But the level of pain, frustration, and efficiency with how they are presented and brought to closure can and should be controlled.

Alignment with your internal stakeholders, such as Legal & Operations, on who is accountable for ensuring a security addendum gets added and communicating that to your vendor is critical. For existing relationships the ultimate success of risk reduction within that relationship starts with understanding your greatest leverage point in the relationship. Is that the relationship itself? Is it based on the disproportionate amount of revenue you provide them? Is it more strategic in nature in how you support their product roadmap and market exposure?

Understand those items and start there in convincing the internal stakeholders, and ultimately the vendor partner, in how to go about implementing the risk remediation program. Often this messaging is better received by the vendor from their known and trusted stakeholder internal to your business than it is from an impersonal 'security function' that can be ignored if not perceived as influential enough to effect change in the business relationship.

Understanding Leverage

The first thing to understand in the process represents that leverage is a very real dynamic. Large enterprise organizations, even if a 'vendor' to you, are unlikely to sign binding security contractual documentation or complete overly customized security risk assessment questionnaires or activities. It's understandably worth the effort to send these requirements over to them, but do anticipate how you will respond when that partner refuses to comply.

Are you going to stop using Microsoft products, or force a platform change away from SalesForce? Likely not. You simply don't have the leverage, and even if you did they are going to mature their risk posture to the degree and at the urgency that they deem appropriate.

Ironically, leverage can work both ways. A more complex problem may be existing smaller business partners who are reluctant to comply simply because the cost of meeting this new set of requirements is exponentially greater than the totality of revenue they receive from your organization.Remediation efforts that require high capital investments and lengthy timelines that shift the focus and priority of their limited personnel resources may be met with frustration. This partner may simply decide to not comply and wait until their contract runs out and terminate the partnership based on the grounds that you have materially and arbitrarily changed contractual terms with costly remediation requirements to the point where it costs them more to do business with you than it does to lose your business. This is not at all problematic if they are providing a replaceable service. And in fact it further supports the value of a third-party risk management program. But what if they are boutique & irreplaceable? Navigating this scenario requires pivoting the discussion to internal leadership stakeholders to align on risk tolerance.

At the end of the day, bringing existing vendor partners into compliance is very frequently perceived by that vendor as 'changing the rules' of how business is, and has been, conducted. Mature organizations recognize that information security requirements are constantly evolving, as are associated regulatory requirements. But less mature partners may be confronted with a problem that is too big for them to fix. At least, not without support from your organization. Getting to the point of tangibly reducing risk in these situations is a narrative that is likely more about understanding and navigating internal and external relationships as it is about handing over a findings report and expecting rapid changes.

FUTURE BUSINESS GROWTH ALIGNMENT PHASE

Align Security Mission to Business Growth Drivers

A direct benefit of the TPRM discovery is providing full visibility into the various efforts and initiatives going on throughout the organization. Executed properly this visibility should provide a starting point for dialogue with key stakeholders to align on priority for how to address vendor remediation efforts based on risk and business need. Structured properly the TPRM program will function proactively as a critical stakeholder in new business initiatives, the pursuit of new verticals, and M&A efforts.

As the organization becomes more accustomed to engaging with the TPRM program it will hit a scalability tipping point. Departmental key players such as those in Project Management, Procurement, Legal, Growth, and Operations will begin to understand the fundamental requirements of the program and begin ensuring that those fundamental requirements are met by any newly introduced entity before they are even presented to the TPRM program for evaluation. Additionally, these key stakeholders will know to pull the TPRM program into the discussion in very early stage initiative discussions to ensure that there are no 'long pole in the tent' concerns that will prevent the initiative from launching on time. This dialogue creates an opportunity to transition the program's perception from a rigid inflexible (but necessary) inhibitor, to a deeply embedded business partner that is partaking in the risk acceptance discussion.

Speed to Launch New Partnership Verticals

A typical business stakeholder fear is that while a TPRM program will assuredly reduce security risk, it will also introduce bureaucracy and complexity that will inhibit the business from moving at the speed it needs to remain competitive. This can be especially true when working with SMB partners who typically have non-existent or immature security programs. and Subsidizing for SMBs can provide competitive advantage.

For example, for an early stage pilot project the TPRM might authorize the business to move forward with a risky vendor for a short period of time to test out viability of the project concept, but set expectations with the stakeholders that the vendor will be required to hit certain levels of maturity at certain timelines or milestones before the project can fully go-live with sensitive corporate data implications. In this manner the project or initiative lead becomes accountable for managing the vendor's expectations directly, rather than having this be a siloed conversation driven by the TPRM program.

Subsidize Remediation with SMB Partners

Another novel and flexible approach to suggest to the key leadership stakeholders is in regards to dealing with SMB partners. The notion is to subsidize aspects of the vendor remediation. This initially seems counter-intuitive on a number of fronts, as the mission of the TPRM program is hopefully to ensure that vendors are at an acceptable level of maturity to begin with. But there is a powerful opportunity to evidence to those stakeholders that the TPRM function can 'think like the business' in an entrepreneurial fashion.

NOTE:

What follows is a later stage maturity opportunity for a TPRM program. It needs to be established and effective, and have secured the funding to have the resourcing to be able to leverage this opportunity.

SMB vendor partners have a unique makeup in that they are small, nimble, and highly innovative in a very specific area. That makeup is what makes them so attractive to the business in the first place, and oftentimes interested business can shape the roadmap of that vendor to it's needs. The downside is that they are typically thinly resourced, and the cost and scarcity of security resourcing frequently leaves satisfying your TPRM requirements beyond their reach. And also, that the cost of implementing the necessary controls may likely require an investment that exceeds the revenue opportunity presented to the vendor. The good news is that where there is chaos there is opportunity!

An innovative TPRM program can (and should) alter its approach in these cases. It is very easy to quickly determine that there is effectively no security program in place. So, alter the assessment strategy from large questionnaires to a more consultative approach. Remember that one of the greatest traits in these SMB relationships is that they are nimble and can implement change quickly. Typically, you are dealing with one of the most senior stakeholders in that organization, and once they understand the risks in front of them, they are often inclined to rapidly address those risks to the degree that they can reasonably finance them. The other critical consideration is that for these SMBs willingness to remediate is only the first step. They often have to appeal to their own Boards for funding, and this takes time. Additionally, conducting things like penetration-testing and new technical controls implementation take time. Time is the enemy of a business looking to move to market quickly.

And herein lies the opportunity. Where there are costly controls requirements like penetration-testing, implementation of technical controls like NGFWs and MSSPs, there is an opportunity for the TPRM program to subsidize these high-end costs, under business negotiation terms. Additionally, this reduces the time necessary to identify penetration-testing contractors or go through technical vendor selection. The TPRM program can directly apply resources to this in near-real time. Perhaps the vendor reduces pricing to offset the cost investment by the business or commits to self-fund controls implementation at certain revenue milestones. These are just examples, but they highlight an opportunity to ensure that fast-track critical business initiatives can move forward at a collectively understood level of temporary risk without sacrificing things like speed-to-market.

Additional benefits of this approach are that the TPRM program can control the quality of things like penetration-testing, while also ensuring full visibility to the resulting reports. Similarly, the TPRM program can ensure that not only was the NGFW purchased, but that it was implemented correctly. And all of this is ultimately sound investment for the vendor in question. This approach facilitates strong transparent relationship development between the business and the vendor. And this, in and of itself, solves the problem of reluctant vendor transparency in risk assessment questionnaires where there is ultimately a fear of losing the business opportunity due to inadequate security posture.

In this manner there are multiple opportunities to collaborate with internal operational and financial stakeholders to develop a cost-model that achieves all goals – Tangible risk reduction, speed to market, and strengthened transparent partnership relations! That is an approach that appeals strongly to most executive leaders.

CALCULATING RETURN ON INVESTMENT

Contributors: Bob Turner and Al Ghous

The cost of managing a TPRM program could be as simple as the labor for a risk analyst to perform the required discovery and analysis. In the report "Third-Party Cyber Risk: 8 Key Considerations" by TPRM vendor RiskRecon, suggests using the cost of the vendor questionnaire as one measure. Using the number of vendors per analyst and the number of questions per artifact, and accounting for surveys taken across multiple industries, the cost per assessment varied between $3,288 (Finance) and $1,805 (Technology). Of course, this number is predicated on the fact that your company performs a large number of these assessments and in a consistent manner.

Using the FAIR Institute's Return on Security Investment (ROSI) calculation (Ref m.):

$$\text{ROSI} = \frac{\text{MONETARY LOSS REDUCTION} - \text{COST OF THE SOLUTION}}{\text{COST OF THE SOLUTION}}$$

You may find the return for conducting a single assessment could be extraordinary while an engagement involving 100 or more components may change your confidence in doing the task.

STAFFING IMPLICATIONS

Contributors: Marc Crudgington and Al Ghous

Without question, some of your staff will be taxed with the implementation of a TPRM Program. The stakeholders involved and the operating procedures of the Program will depend on the size of the organization, number of vendors, and organization structure. You may even find it necessary to hire additional staff depending on the size required to implement and manage a Program. Certainly, look to gain efficiencies where you can with technology and well-defined processes and procedures, but there will be additional tasks staff will be assigned and a Level of Effort (LoE) required to operate and maintain a program, even if the majority of it were outsourced.

Provided next is a perspective of the time it may take staff to procure a vendor that is rated at a moderate level; you can add or subtract time based on complexity of the vendor and contracts. Some tasks will take the same amount of time regardless of vendor complexity. We have not allotted time to conduct required Proof of Concept/ Proof of Value or on required Penetration Test; those tasks are too arbitrary to put a time limit on.

Alternatively, some of the functions in the table to the right can be conducted by acquiring a Third Party Risk Management product that provides Managed Services. In this model, the solution provider or vendor will perform one or more of the core TPRM functions.

SAMPLE TIME REQUIRED FROM STAFF IN REVIEWING A VENDOR

GENERAL COUNSEL
NDA Review (Creation)
3-4 hours
Initial Review
0
Periodic Monitoring

GENERAL COUNSEL
Contract Review
4-6 hours
Initial Review
0
Periodic Monitoring

VENDOR OWNER SPONSOR
Initial Vendor Forms
1-2 hours
Initial Review
1 hour
Periodic Monitoring

VENDOR MANAGEMENT OFFICER (PROCUREMENT)
Ensure all required forms and process is complete
4-6 hours
Initial Review
2-3 hours
Periodic Monitoring

CHIEF INFORMATION OFFICER
Technology review completeness
1 hour
Initial Review
<1 hour
Periodic Monitoring

CHIEF INFORMATION SECURITY OFFICER
Security review completeness
1 hour
Initial Review
<1 hour
Periodic Monitoring

TECHNOLOGY REVIEW
Review architecture, demos, technology stack, etc
4-8 hours
Initial Review
1 hour
Periodic Monitoring

SECURITY REVIEW
Review security architecture, demos, security documents, perform assessments
6-10 hours
Initial Review
3-4 hours
Periodic Monitoring

COMPLIANCE
Review contract/ relationship for compliance ramifications
1-2 hours
Initial Review
<1 hour
Periodic Monitoring

VENDOR MANAGEMENT STAFF (PROCUREMENT STAFF)
Input vendor in system, assist Vendor Management Officer
3-4 hours
Initial Review
2-3 hours
Periodic Monitoring

FINANCE
Accounts Payable
1 hour
Initial Review
<1 hour
Periodic Monitoring

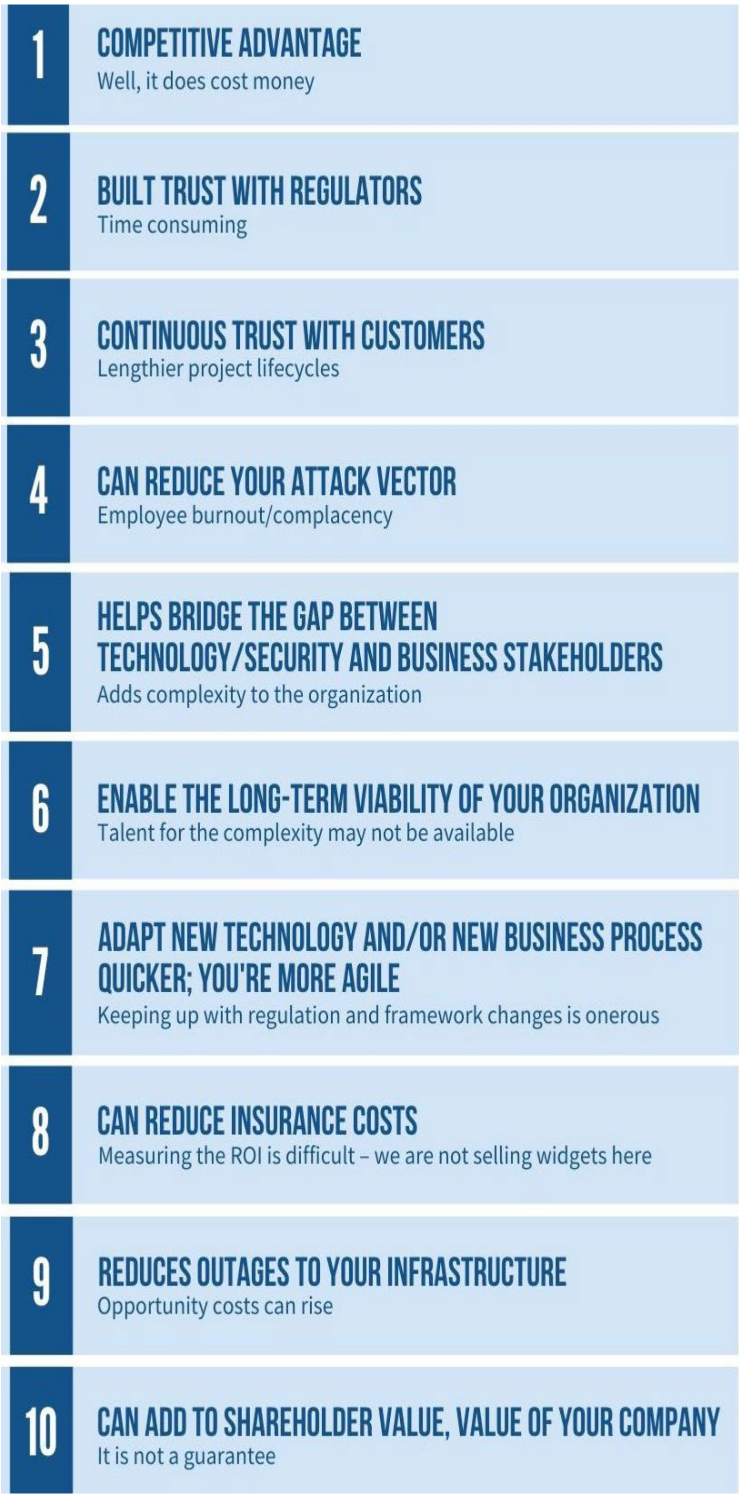
EXECUTIVE MANAGEMENT
Sign-off on vendor, review vendor(s) in meeting
<1 – 1 hour
Initial Review
<1 hour
Periodic Monitoring

VENDOR MANAGEMENT COMMITTEE
Review vendor(s) status, overview of vendor
<1 – 1 hour
Initial Review
<1 hour
Periodic Monitoring

MAINTAINING COMPLIANCE

Contributor: Marc Crudgington

As we discussed in the section Relationships to Frameworks and Industry Resources, following laws and regulations for many industries is mandated. With those organizations where data, especially privacy data, is the new gold, many privacy laws may inherently be part of your cybersecurity program and business operations. The more you engrain processes to help adhere to these laws and frameworks and automate them, the better off your organization will be. It goes without saying that this is much easier said than done. Applying sound security principles to the process requires work and continuous diligence to maintain compliance. Third-party risk management is no different. The more complex your organization, the more third parties you may have causing you to evaluate them with the frequency based on how you have defined them in your program. Adhering to strong third-party risk management principles will only help you maintain compliance with necessary regulations or adhere to required standards. Many of the laws or standards have within them sections of requirements governing third-party risk management. Developing repeatable processes from sound frameworks will only help your organization be more consistent in its approach and maintain the hygiene required.



1 **COMPETITIVE ADVANTAGE**
Well, it does cost money

2 **BUILT TRUST WITH REGULATORS**
Time consuming

3 **CONTINUOUS TRUST WITH CUSTOMERS**
Lengthier project lifecycles

4 **CAN REDUCE YOUR ATTACK VECTOR**
Employee burnout/complacency

5 **HELPS BRIDGE THE GAP BETWEEN TECHNOLOGY/SECURITY AND BUSINESS STAKEHOLDERS**
Adds complexity to the organization

6 **ENABLE THE LONG-TERM VIABILITY OF YOUR ORGANIZATION**
Talent for the complexity may not be available

7 **ADAPT NEW TECHNOLOGY AND/OR NEW BUSINESS PROCESS QUICKER; YOU'RE MORE AGILE**
Keeping up with regulation and framework changes is onerous

8 **CAN REDUCE INSURANCE COSTS**
Measuring the ROI is difficult – we are not selling widgets here

9 **REDUCES OUTAGES TO YOUR INFRASTRUCTURE**
Opportunity costs can rise

10 **CAN ADD TO SHAREHOLDER VALUE, VALUE OF YOUR COMPANY**
It is not a guarantee

There are benefits and costs to following a framework, adhering to mandated laws or industry requirements, and/or having sound cybersecurity hygiene. By no means are the benefits and costs listed on the preceding page exhaustive; you may realize more benefits and costs based upon your organization’s effort.

Let’s face it, we all may want what the Joneses have, but we may not be willing to work as hard or sacrifice as much to realize it. Yes, getting and staying compliant is hard work. Whether that is following regulations your industry requires, following a framework, or just simply practicing ‘best of class’ cybersecurity hygiene. Third-party risk management is no different; it takes repeatable processes that get validated through framework assessments or other assessments which demonstrate you are following guidelines and best practices.

Though it can be difficult, the burden can be lessened by following a known framework, whether one or a hybrid approach, and adopting a continuous cyber-hygiene lifecycle. Adopting a continuous compliance mindset such as Gartner’s CARTA or any of the other maturity type models can help an organization easily adapt to new laws, new risks, and be ready for new operational business challenges.

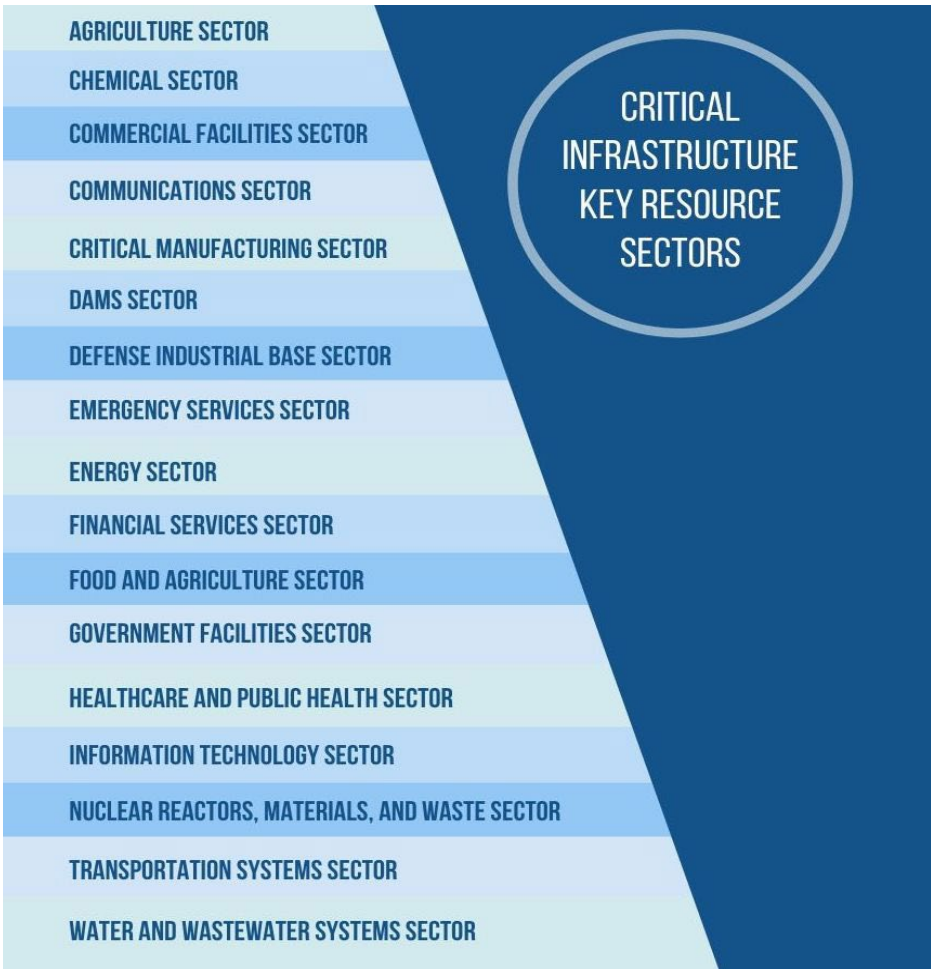
BEYOND SECURITY: OTHER BUSINESS CASES

Contributor: Mike Davis

There are a few ways to depict the potential business and industry use cases where TPRM effectiveness can be a significant organizational issue to accommodate. One example is to take a "CIP" view (Critical Infrastructure Protection). Just what is "CIP" and what key industries are considered most essential varies.

Presidential Policy Directive 21 (PPD-21) addresses Critical Infrastructure Security and Resilience and provides a national policy to maintain secure and resilient critical infrastructure and identified 16 critical infrastructure sectors. All CIP sectors fundamentally need to use TPRM for the same reasons as captured above, minimize down stream data breach and privacy violation risks; whereas the impact of a CIP sector being degraded is much more impactful to the community at large than just one organization being compromised. Many of those also have a higher propensity to have a human casualty impact.

Table: Critical Infrastructure Key Resource Sectors



CRITICAL INFRASTRUCTURE KEY RESOURCE SECTORS

AGRICULTURE SECTOR
CHEMICAL SECTOR
COMMERCIAL FACILITIES SECTOR
COMMUNICATIONS SECTOR
CRITICAL MANUFACTURING SECTOR
DAMS SECTOR
DEFENSE INDUSTRIAL BASE SECTOR
EMERGENCY SERVICES SECTOR
ENERGY SECTOR
FINANCIAL SERVICES SECTOR
FOOD AND AGRICULTURE SECTOR
GOVERNMENT FACILITIES SECTOR
HEALTHCARE AND PUBLIC HEALTH SECTOR
INFORMATION TECHNOLOGY SECTOR
NUCLEAR REACTORS, MATERIALS, AND WASTE SECTOR
TRANSPORTATION SYSTEMS SECTOR
WATER AND WASTEWATER SYSTEMS SECTOR

The Department of Homeland Security (DHS) lists 19 groups of sectors as Critical Infrastructure Key Resources (CIKR) such as: Water, Emergency Services, and Healthcare and Public Health (HPH).

Then there is a "lifelines" approach (critical services) centered on localities / counties with four main categories that apply to almost every county:

- Energy, such as oil, natural gas and electricity,
- Water, including potable water and wastewater systems,
- Transportation, including roads, bridges, rail, airports and ports, and
- Communications, including telephone, satellite and Internet infrastructure.

So what really matters in CIP? The CIP industry based business / use case for TPRM is fundamentally based first around availability (the "A" in C.I.A triad of cyber security), followed by assurance (is this entity who they claim to be?) – especially for those 'lifelines' industries. While they all need to have an effective TPRM as a business themselves, they are in the supply chain of virtually all other business; thus indirectly a critical 3rd party for all of us (as doing without one of them, like communications or power, can put us out of business if we don't at least consider alternatives in our risk assessments). So clearly most businesses won't ask the national providers to respond to a questionnaire (though the local extensions you likely would – like your WAN provider / ISP); yet account for them you must. We recommend a CIP section in your TPRM that addresses and quantifies this support aspect, ending with what providers you will assess, then track them like all the others.

Current Statistical Thoughts

Sample TPRM program factoids…

While the downside of NOT doing TPRM is substantial for most organizations, just what are the costs, issues, et al? While there are many good articles on this aspect, we highlight one in particular, which has a mix of facts / figures and just a little FUD for good measure. (Ref q.)

When it comes to vetting and evaluating third parties:

- Third parties are inundated --- 15,000+ hours spent on completing assessments each year
- Enterprises aren't getting insights --- 54% say data is only somewhat valuable and less than 8% of assessments result in action
- The cost of failure is high --- 70% believe cost of failure is $13 million (costs include impact on reputation and brand, decreases in share value, loss of business, etc)

Overall statistics:

- $2.1 million is the average annual spend on vetting third parties. Surveys show that 64% say the processes used are only somewhat or not effective
- 40% of organizations use manual procedures, like spreadsheets and 51%

employ risk scanning tools, to vet their third parties. In fact, 34% said results of these tools are only somewhat valuable while 20% said results don't provide any insights
- Third parties are spending 15,000 hours a year on completing assessments, at an average cost of $1.9 million annually. Over 55% said these assessments only somewhat or do not accurately reflect their security posture
- Only 8% of assessments result in action (eg. disqualification of a vendor or a requirement to remediate gaps).If assessments revealed gaps, only 26% of respondents say their organizations terminated the relationship

These are the biggest takeaways for key decision makers:

- Current practices and technologies used to support TPRM and assess third parties are costly and often inadequate and inefficient.
- Investing in better assessment and vetting tools can increase effectiveness in TPCRM while decreasing the cost of maintaining the program.
- Applying the same approach to all third parties can be costly. Taking the time to prioritize third parties and apply an appropriate level of due diligence to them will reduce costs and increase efficiencies in the long run.
- Control over budgets for third-party cybersecurity risk management is dispersed throughout the organization which can make the allocation of resources inefficient because of management interests in the various functions

ONE VENDOR'S PERSPECTIVE

Many CISOs have partnerships with vendors that go beyond the contract in place. The best relationships are where the CISO and vendor can talk openly about their challenges and solutions. While there are many vendors in the TPRM space, we asked Black Kite to provide some of their thoughts on TPRM that are not always part of the sales pitch.

Contributor:
Bob Maley, Chief Security Officer of Black Kite

The CISO's Changing Role

Historically, the CISO has primarily focused on the cyber risk of their enterprise, systems and data. A steady, but increasing move to outsourcing everything from servers, software development and enterprise platforms now requires a CISO to expand their focus to an enterprise ecosystem.

The CISO is also being asked to oversee cyber assessments of third parties. The TPRM stakeholder community includes others such as business units, procurement, legal, compliance, finance and risk. This additional involvement can become challenging for the CISO, as each stakeholder may have a different process or language to assess a third party.

One example is the phrase "concentration risk," defined as the use of a single, or small pool of vendors for critical processes. Concentration risk assumes if one vendor fails, the negative impact can be drastic. Procurement may look at vendors through the lens of "spend", assuming the more money a vendor receives, the more valuable the service must be. The CISO tends to talk about "cyber risk" in qualitative terms of high, medium or low, based on evaluations of controls that are deemed relevant.

The first challenge for CISO's is the difference in what stakeholders view as risk, and the second challenge is the ability to scale the process of assessment. When a CISO is protecting their own environment, they may look to a framework such as NIST 800-53, implementing and testing many of the suggested controls; which, in a high-risk environment, can add up to as many as 200 controls. When a CISO evaluates hundreds of vendors that will have access to data and systems material to a business, the scope of assessing that larger ecosystem multiplies to thousands of relevant controls.

A cyber security TPRM program that tries to review large volumes of data quickly can find itself overwhelmed. The use of real-time questionnaires have value in baselining new vendors, but can quickly become out of date from an ongoing risk management perspective. The use of continuous monitoring solutions that report on thousands of potential vulnerabilities can also cause a TPRM program to implode. In order to create a TPRM program that truly brings value to the organization, the CISO must break out of the cybersecurity box and begin to think and speak in the terms a business best understands, and that is usually in financial terms.

Initial Steps

The first step is to use the same definition for risk across the business. Many organizations use the Open FAIR© (Factor Analysis of Information Risk) framework. The framework calculates "the probable frequency and probable magnitude of future loss associated with a specific event," or in more simple terms, the economic impact of a cyber event.

The next step is to review how you classify or tier your vendors. Many CISO's will use the high, medium or low approach, or Tier 1, Tier 2, etc. This normally correlates to the classification of data a vendor has access to; for example, a Tier 1 vendor has access to Personally Identifiable Information (PII). The challenge to this methodology stems when translating the tiers into probable financial impact. If done at all, this translation is done using opinion, ranges that introduce error into results and messaging that other stakeholders either don't understand or have no verifiable track record of results.

To move to an economic (financial) impact model, the CISO must step outside of the cyber security box. This economic impact model is also built from classifications; however, is more sophisticated based on quantitative relationships to risk. Vendors are classified by a number of key factors and, for the purposes of this overview, the risk focus is cyber events.

First, identify every vendor you share or grant access to confidential data (this can be PII, payment transactions, etc. – you can add as many classifications to align with your business model). Next, classify types of network access, e.g., does the third party have persistent access to your network? Then, focus on vendors deemed "business critical", because regulatory requirements may demand specific actions such as continuous monitoring. These vendors are likely the same group of third parties where you are currently conducting extensive assessments.

The next step is to conduct a quantitative risk assessment on this pool of vendors. If you choose a manual process (such as the one outlined in Hubbard's "How to Measure Anything In CyberSecurity Risk"), start with an existing classification of 'high' or 'Tier 1'. If the organization's enterprise risk management team has quantitative analysis experience, you may want to engage that team as they may have leveraged technical and process automation in the past.

Another option is to use Black Kite's 3D Vendor Risk@Scale^{SM} platform, which automates the collection and calibration of each breach, threat, vulnerability, and numerous other data points used in the quantitative process. This approach will bring you closer to the goal of gaining an understanding of the potential economic impact of events occurring with your third parties. The information garnered from this platform provides the output required to make risk-based (economic impact) decisions concerning which third party risk management activities should be applied to a particular third party.

Achieving A Risk Based Approach

The level of effort invested in the steps outlined above move you to a true risk-based impact view, versus a classification-based approach to risk management. With this information in hand, you can improve your understanding of third party risk by aligning third party engagements to the corporate risk appetite (see note) or risk tolerance levels. Every business will have a different view on what risk level they are willing to accept in order to conduct business.

Regardless, making steps in this direction is essential to completing the decision-making loop. When you understand the organization's risk appetite, or the extent in which a business is willing to tolerate engagement with a vendor, you are in a better position to make informed decisions. You will also be in a position to know where to invest precious TPRM resources, reducing the uncertainty of your risk exposure.

Note: We will not go into the process of determining risk appetite in this paper, as there are numerous excellent resources already available. Douglas Hubbard's "The Failure of Risk Management - Why It's Broken and How to Fix It" is one of the best pieces on the subject and details defining risk appetite, the value it presents in analysis and how to effectively discover the information in your organization.

In a perfect world, every third party's risk would fall at or below your organization's risk tolerance, a necessary goal for your program. In reality, a classification-based risk program doesn't connect with or reflect your business goals; rather a classification-based risk program is a qualitative attempt to show some type of risk metrics. By establishing a connection to corporate risk appetite, you can make decisions that meet business needs. If your program has not yet matured to this stage, there are still things you can do to reach your business criteria and overarching goals.

Managing Risk

Corporate risk appetite combined with building a process based on impact level can be ranked on a scale as follows:

1. at or below risk appetite,
2. within risk tolerance, or
3. over risk tolerance.

When the economic impact is expressed as falling within one of these three distinctions, a specific workflow can be initiated to quantify potential impact.

For example, if the impact is at or below risk tolerance, then follow a specific set of actions, such as:

- Monitor events that would raise economic impact levels beyond tolerance
- Perform a specific periodic review (such as an annual questionnaire or artifact collection
- Acquire cyber insurance to cover the potential impact
- Execute other actions that may be classification specific
- In the event a third party is above risk tolerance then follow the below actions:
- Conduct a more thorough assessment that may include an onsite visit, penetration test, third party certification, etc.
- Conduct internal reviews on the engagement model for remediation (e.g., Lower number of records shown, disallow network connection. etc.).
- Review the cyber hygiene of the third party to identify items that if remediated would reduce economic impact
- Undertake other actions that may be classification specific
- A process for those third parties above the risk appetite but within risk tolerance could also trigger a set of predetermined actions, such as:
- Collect control questions to enhance the accuracy of the impact assessment to determine if impact raises or lowers
- Continuously monitor the third party for changes to posture
- Acquire cyber insurance to cover the potential impact

Next Steps and Recommendations

These actions are purely suggestions, and your process should be determined by your business requirements including internal policy, regulatory requirements, and corporate culture. If you are unsure of what best practices to follow, there are a number of resources available such as https://sharedassessments.org/ which includes a wealth of studies, white papers, industry knowledge and tools. One very important tool is the Vendor Risk Management Maturity Model Tool (free at the site).

If you are still in the process of understanding your corporate risk appetite, other sources of information are available. Third party engagements that meet the classifications outlined above most likely have information obtained in the procurement process, which can be used until the risk appetite becomes understood. Often, a business impact analysis may have been conducted, or a cost-benefit analysis is available. This information can help you reduce the uncertainty surrounding the risk profile of a particular third party.

As an example, a vendor whose cost-benefit analysis reveals the value of the engagement is far less than the potential loss or economic impact, can help drive engagement within the business and create an understanding around what may be an acceptable loss.

Using a true risk-based approach, one which moves beyond classification and provides an economic impact perspective of profit and loss for each unique vendor or vendor type, puts you on the same page as the business. Terms like "high cyber risk" or "insufficient technical scores" for a third party can create churn and resistance from the business side. After all, while your focus is risk management, their focus is conducting business and generating profit. Colleagues responsible for cost-benefit analyses will be very open to a risk based approach when you propose requests for support, as opposed to the security department knee-jerking response that is often received when requesting resources – an emphatic "NO."

Once you build a mature third party risk management program based on risk, you will have a program understood by the board, in line with business goals, and defensible to any auditor or regulator.

MARKET ASSESSMENT

Contributors: Al Ghous, Joey Johnson, and Bob Turner

Major Features

TPRM is a critical aspect of any successful Security program. It continues to increase in importance as legal, sourcing, procurement, security, risk, privacy and compliance leaders look to improve their response to increasing regulations, greater scrutiny from their customers, program efficiency and risk reduction. This notion is not new by any means and the Security vendor community has taken notice by introducing a growing list of products and services. It became important enough that Gartner developed a Magic Quadrant for it, called Vendor Risk Management.

As CISOs and other Security practitioners navigate the marketplace, one will find that there are several approaches to assessing third party risk. Based on today's landscape, we see the industry solidifying on three different approaches for which there are countless solutions – enough to cause confusion.

Traditional Third Party Risk Management: This category of solutions come with traditional Governance, Risk and Compliance (GRC) products. They provide workflow to send questionnaires to vendors, assess risk, manage remediation and report out. The customer would manage the inputs and outputs.

Managed Services Based Third Party Risk Management: This category is somewhat similar to Traditional Third Party Risk Management solutions, but in this case the vendor would provide managed services to perform some or all of the customer's third party risk management activities such as sending questionnaires and tracking remediation. Furthermore, the managed services would perform some or all of the inputs and outputs.

Third Party Risk Management With Security Scoring: Similar to Traditional Third Party Risk Management but with capability to provide assessment data and/or other vendor risk supporting content in support of third party risk assessments. The common data that is provided is a score, whether it is rating the security posture or risk of the third party.

It is important to note that although a vendor might focus heavily in one category, the observation of today's solutions indicate that the lines are being blurred and more and more vendors are aiming to provide a more comprehensive platform that can support all of the aforementioned approaches as well as providing other GRC related solutions. Some emerging solutions are even including audit support and support for continuous compliance [operations] and assessment.

Analysis of vendor responses to the CISOs Investigate: TPRM RFI

General: All solutions offer automation and data visibility which provides great insight on the supply chain vendor approaches to security and risk. All solutions share data with the third party vendor being assessed which is great for transparency, though it may cause the party assessing risk to have more restrictive data management chores if an assessment responses are retained.

Specific CISO feedback included:

Mandatory Requirements (Must Have)

- Risk scoring frameworks are important. Only two of four providers stated they use a specific framework.
- All solutions share data with the third party vendor being assessed.
- All solutions provide digital footprinting though the details would need more clarity for that data to be useful.

Additional Requirements (Preferred)

- CISO analysts noted that it would be a huge time saver if the platform can support controls based questions from Cloud Security Alliance (CSA) or other standards bodies.
- Vendors should provide a more customizable risk scoring methodology that fits the customer's internal risk assessment and scoring model beyond what NVD provides.
- The ability to provide a vendor's score and posture relative to other companies, but more importantly their own industry, is a very effective measurement tool.

General Business Requirements

- Dependency mapping that is very specific to the customer and their vendors, and their vendor's third parties (customer's fourth party) as sub processors is key to understanding supply chain risk. Hard to tell if any of them do this kind of mapping. Ironically each customer will most likely know their vendor's sub processors via their MSA. It's usually listed there.

General Technical Requirements

- None of these vendors seem to do a good job with elastic IPs provided by public cloud providers.
- Many of the responses show the vendor community is API driven with some of the CISOs concerned about how those APIs are to be managed.
- External vulnerability scans are done on their own. They expose APIs for third party tool integration like GRC, etc.
- Half the solutions are RBAC focused (seen as a plus)

Most of these platforms were assessed as weak when it comes to describing their workflow for their customer's vendors to exclude items that are a first party responsibility or the vendor is not able to verify.

TOP 10 KEY TAKEAWAYS

Contributor: Mike Davis

Congratulations on making it this far, or did you just skip to the end (you A+ types!). Assuming you realize the criticality, necessity and even legality to have a TPRM program of some type, the table below provides a high level view of the top activities and/or risk value decisions that must be part of your TPRM effort.

FUNCTION	DETAILS	COMMENTS
1 COMPLEXITY	TPRM efforts will only grow in types / volume of risk areas How will we keep the supply chain security assessed 'everywhere'?	E.g., 5G, IoT, cyber threats proliferation / automation, etc What happens when 3rd, 4th, etc parties loop around and recursive risks dominate?
2 REGULATIONS/ LAWS	Continue to expand and get even more prescriptive – How does anyone keep track, let alone prove compliance	Where / how will the 'risk domino' effect be anchored, shared; whereas the principle party can know, monitor, assess only so much…
3 JOURNEY VS END STATE	TPRM is not a set and forget function set, given the ongoing technical and cyber threat advances as well as increased outsourcing and affiliate partnerships.	Clearly the standard must be continuous monitoring at some level – whereas this risk could well be the largest for the organization
4 ALL ABOUT ERM	TPRM is but a part of the overall enterprise risk management effort, yet a major liability in some cases, it must be visible top down	Starting with a top down approved risk appetite… easy to say, harder to get a documented statement in play
5 PERFORMANCE TOO	Risk is the focus but SLAs, performance metrics – both for the risk mitigations and overall service responses should be in here too	Best to keep these two as one assessment, as a low risk with poor performance is also a termination factor. Service interrupts and upset customers are reputation busters.
6 DATA QUALITY	It depends on what type of questions you ask and how they are interpreted – thus responses can vary a lot, making assessments problematic	Start with an accepted assessment, like the Standard Information Gathering (SIG) questionnaire from Shared Assessments or other standard survey form
7 AUTOMATION	Not only automating the process, inputs, reminders (aka, "GRC" like functions), but pre-populate fields, etc	The monitoring functions need to be likewise improved to verify the automated functions, error checking, etc
8 ENVIRONMENT CHANGES	Entities continuously improve and change their services, capabilities – these need to be captured and assed	Ideally 3rd parties have a change notice process and you include that process in your contracts.
9 SUPPLY CHAIN	Along with complexity, this risk is also expanding. Including capability risks that maybe several parties have at the same time.	Few have an effective supply chain risk policy / standard to start with (do you?), while this may be principally performance based, there are many shared risks as well
10 AI/MI/BLOCKCHAIN	How will technology advances affect what TRPM assesses?	e.g., assess automated, secure, distributed ledgers / contracts

SUMMARY

In effect, you are betting the business livelihood and even organizational existence by NOT having a 'reasonable security' posture that includes an effective TPRM plan - whereas it is the cause of over half of all data breaches. Given the key takeaways and other recommendations in several sections, this summary is then a further distillation of those points.

- It's all about RISK of course, so relate TPRM to key business success objectives, use KPIs.
- Our interconnected environment will get more complex, but don't delay - get a TPRM program started asap, iterate as you learn more and mature the processes.
- A contract management system is foundational, automation is key too, and then only collect the data you can use, make decisions with. Spend time on whittling down your list up front.
- TPRM does not stop at the 3rd party level. Significant risks are in the 3rd party connections and beyond – so follow those trails too.
- It all starts with a detailed, approved policy that is well communicated. If folks can get a contract in place before the TPRM process is used – you lose. Get the CFO on board as the gatekeeper!

TPRM, it's not just another check in the box, it's your career and livelihood!

MARKEL CORPORATION

PATRICIA TITUS

Chief Privacy and Information Security Officer

REAL-WORLD CASE STUDY
THIRD PARTY VENDOR RISK MANAGEMENT

CHALLENGES

Markel Global Security Services (GSS) wanted to enhance, but also simplify the approach to the Third Party risk management process. The current process was very manual, cumbersome and was unmanageable by the team.

APPROACH

In 2017, GSS planned a 'shark tank' like event, inviting 32 companies to pitch their products for 20 minutes to the GSS team. The team then took the top five vendors and allowed them to do a deeper dive, possibly being considered for a formal relationship.

Black Kite had just graduated from a cyber security incubator when they presented to GSS their tool. What was shown was a perfect cyber risk rating platform that leveraged open-source intelligence and non-intrusive cyber reconnaissance scorecard.

SOLUTION

Markel performed an assessment of all scorecard vendors, finding Black Kite's cloud-based solution to be the best and most mature. The easy-to-use dashboard makes it simple to explain risk to any business leader or executive. GSS has found that Black Kite's approach to Third Party due diligence creates an easy, consumable way to manage hundreds or thousands of Third Parties at scale. New enhancements have led to a more robust reporting capability as well as delivered a new 'continuous monitoring' feature at no additional cost. Alerts can now be set, which trigger when possible issues with a 3rd party are seen. In the latest releases, Black Kite has introduced the Factor Analysis of Information Risk model, or FAIR for short. This model, which is used to calculate the probable financial impact if a Third Party experiences a breach, in easy to understand business terms. Based on the incorporation of FAIR, as well as other improvements within the tool. Of course, all this information still has to be analyzed by our Risk Management team but has automated a large part of our analytic process.

BENEFITS

Black Kite continues to be a partner with a great value added proposition. We've been able to manage costs through our unlimited licensing, which makes budgeting consistent year over year, and we still get all the enhancements at no additional cost. Plus, because of the addition of the FAIR Model, we can help our business customers make decisions with enriched risk data by providing the whole picture. This tool is a great start to the journey of moving away from relying solely on questionnaires.

CISO CONTRIBUTIONS

ALLIANTGROUP

LEVI STRAUSS & COMPANY

HELLMAN & FRIEDMAN PRIVATE EQUITY

H.I.G CAPITAL

NEXTEER AUTOMOTIVE

PREMISE HEALTH

RICOH USA, INC.

RWJBARNABAS HEALTH

SERVICEMAX

UNIVERSITY OF WISCONSIN - MADISON

WOODFOREST NATIONAL BANK

ALLIANTGROUP

MIKE DAVIS

Chief Information Security Officer

COMPANY OVERVIEW

alliantgroup is a consulting firm that offers best-in-class resources to accelerate growth for U.S. businesses both domestically and abroad. We combine these resources with insights from our expert advisors to provide industry specific consulting in key business areas such as management consulting, risk advisory, tax, cybersecurity, technology and talent. We are proud to have helped 18,000 businesses claim nearly $10 billion in tax incentives. We partner with more than 4,000 CPA firms, have completed more than 50,000 studies, and have helped create more than 165,000 jobs.

With 1000 professionals on staff and growing, alliantgroup is the only provider in the country with architects, engineers, software developers, agriculturists, PhDs, scientists, tax specialists, former 'Big Four' accounting firm executives, former Secretaries and members of Congress, CPAs and more. Our unique model offers clients unmatched expertise marrying industry knowledge with the complex requirements of the tax code. alliantgroup was founded in 2002 and is headquartered in Houston, Texas with additional offices located in Austin, Boston, Chicago, Indianapolis, New York, Irvine, Sacramento, Washington, D.C.; and Bristol and London in the U.K.

BUSINESS USE CASES

alliantgroup works with thousands of CPAs so it is imperative that we manage our third-party risk. From a big picture perspective, we are concerned about Third Party Risk Management (TPRM) as a process to minimize the overall data breach risk surface. We also want to ensure operations from a technology standpoint.

Much of what alliantgroup does requires conforming with financial and privacy regulations. However, TPRM covers much more than compliance with industry statistics indicating that over half of a company's risk exposure to data breaches comes from third parties. In addition to all of the regulations and laws covering data breaches and privacy violations that we adhere to, our business in large part supports CPA firms who trust us as a steward of their data; so for all intents and purposes we also function as a third party and are very aware of that and what safeguarding against third party breaches requires.

We segment our TPRM policy into two elements: companies that handle any sensitive data and other that provide technology services. In security vernacular, the data component covers confidentiality, integrity and availability and for technology partners it is more about availability. We categorize third party partners as being "critical or important". Companies that handle any sensitive data are automatically classified as critical as well as those who can significantly impact availability of our services. Important companies are then those who could have a noticeable availability impact, but we could find alternative services for.

BUSINESS GOALS IMPLEMENTING THIRD PARTY RISK MANAGEMENT

Protecting our client data is paramount to us, not only from an audit and compliance perspective but also from a security and trust perspective. In addition to maintaining strong security controls it is business critical that we are available for our clients. As a SOC2 certified service provider we are committed to maintaining that level of protection while continuing to minimize our overall risk from business partners.

We then meet our business goals of being a trusted partner to our clients by ensuring that our risk of a third-party data breach is relatively low. We do this by strictly limiting the sharing of sensitive data and conducting risk assessments for those partners. This due diligence is imperative as besides data breach risk reduction, TPRM ultimately comes down to minimizing any interruption of business operations.

KEY FACTORS TO CONSIDER

The key for any organization is to understand what their specific business and technology needs are and how TPRM affects those needs. As a medium-sized business we didn't need an overly robust and sophisticated TPRM system. We needed a process that enabled us to be compliant and facilitated the business by safeguarding data and ensuring availability. In addition to our in-house process, we leverage a governance risk and compliance (GRC) tool that handles a variety of functions and grows with our changing needs. Currently, we are focused on compliance as we are working to incorporate the NIST Security Framework and SOC2 audits. An additional benefit of the GRC tool is that other departments can use it for their audits, including but not limited to financial audits. We also leverage this tool to capture the results of internal and external surveys and to keep track of new and ongoing issues and risks (e.g., our enterprise risk register).

Our partner companies fill out the survey to start the process which is followed by a risk assessment we conduct. If there is a concern, we formulate a mitigation and implementation process. The tool then allows us to easily track and follow up. For example, if a partner agrees to implement a fix in three months, a reminder is input into the system for us to follow up to ensure it has been completed.

KEY TECHNOLOGY COMPONENTS

When we decided to investigate various TPRM solutions there wasn't any one technology component 'must have' we were searching for. As a company in a highly regulated sector, our security team built a requirement list that focused on GRC needs and its support for TPRM. We did our research, looking at analyst reports and conferring with our CISO peers locally. We quickly compiled a list of 10 - 12 must-have functional capabilities. That framed our product selection criteria against which we assessed the tools and selected one based on what best fit our technology requirements and the cost. Each organization will have its own short list of needs against which they will conduct a business cost analysis to see which fits their needs and compare the associated costs.

During our research, we found that most of the solutions are cloud based. However, we opted for an on-premise tool because we didn't need to back haul data to the vendor. We did ensure the product could handle the templates we needed to create. The product out of the box had several templates that we use for different reports and compliance mandates like Sarbanes Oxley (SOX) and the General Data Protection Regulation (GDPR). As a bonus, we had them customize a couple of TPRM reports that they were able to do for us within hours.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

Our GRC solution and in-house process have provided us a high confidence that we are capturing and addressing the potential risks while continuing to monitor for any changes. We found that by using a tool we experienced productivity gains as we have decreased the number of emails, meetings and manual tracking – all labor intensive and prone to error. Our tool allows us to add a file or an artifact into the repository that is beneficial in terms of one entry that support both audit and forensics. As well, it allows data to be entered once and accessed multiple times for other audits. We continue to expand our use of the tool for security and privacy tracking in addition to TPRM, while also are deploying it as a company-wide utility. The ability to leverage this one tool for many uses is a big plus for all.

STAFFING REQUIREMENTS

In our experience, there is no question that our TPRM tool saves us considerable time and increases our security team's productivity. In addition to the tools capabilities, during our process and workflow reviews, many manual processes and workflow roadblocks were removed. Less time is spent on back and forth messages about questions related to missed data or what repository something is supposed to be in. We still have to support the audit process and coordinate efforts, as auditors use their own tools, but we can show actual time savings. At a minimum, it allows us to put the artifacts, evidence, and files into one repository where they can be tracked and queried. There is no question that to do TRPM effectively you must use a tool. The GRC tool we selected does what we need and was very affordable.

PEER RECOMMENDATION AND ADVICE

As in every endeavor, you must define your business and technical requirements upfront. You need to establish from the outset a risk assessment process and what matters most to your organization and the risk appetites for each major element. Be sure your key stakeholders agree on the goals of the program and the best way to execute it. I recommend establishing risk assessment process thresholds and mitigation strategies within your ERM and TPRM before implementing them.

Some organizations in less regulated fields may be less interested in a GRC tool and prefer a solution that directly assesses and assigns risk to third party partners. As a company with a very low tolerance for any data or privacy risk, we had to find a GRC tool that enabled us to not only meet compliance mandates but allowed us to effectively assess our third-party risk, as trust and availability is paramount for us.

Depending on your organization, TPRM reports like the one you are reading, will help you determine where to start, because at first you won't know what you don't know and what functions are important when building or enhancing your TPRM approach. Your team needs to create a matrix with your specific requirements as different tools work with different environments. Knowing your company's needs allow you to apply a "Lowest Price, Technically Acceptable" source selection process.

Specifically, for TPRM, it is imperative that your organization already has an effective contract management process to track all contacts coming in and out, in order to determine which of your vendors need to be assessed and if they need to be tracked. If you don't have that fundamental process in play, then you're going to potentially miss some company that could be critical or important to protecting your data and company.

SUMMARY

TPRM is one of the largest potential data breach risk facing companies today. In addition to improving security, having a process, which may or may not include tools, will help improve communications and relationships with your company and business partners as you share both cyber and business best practices. You only can assess what you know exists, while obvious, a complete contract tracking process must be in use and easily able to leverage to mitigate third party risk. Most companies will be unable to effectively conduct TPRM manually. When surveying your partners, keep their end risk posture in mind. Ask only high-risk impact questions. Remember, you have to assess all responses and track whether risks are being mitigated. Use the process to get to know your most critical partners better, share cyber security. In short, you too are likely a 3rd party to someone else so think about how your questions and responses would relate to your own company. The risk assessment and tracking function is critical of course; make that work effectively for you and your partners, they should know what matters from your end as well, and each can likely offer improvements to the other. Putting cyber information sharing in action.

LEVI STRAUSS & COMPANY

COLIN ANDERSON

Global Chief Information Security Officer

COMPANY OVERVIEW

Levi Strauss & Co. is one of the world's largest brand-name apparel companies and a global leader in jeanswear. The company designs and markets jeans, casual wear and related accessories for men, women and children under the Levi's®, Dockers®, Signature by Levi Strauss & Co.™, and Denizen® brands. Its products are sold in more than 110 countries worldwide through a combination of chain retailers, department stores, online sites, and a global footprint of approximately 3,200 retail stores and shop-in-shops. Levi Strauss & Co.'s reported 2019 net revenues were $5.8 billion. The San Francisco headquartered company employs a staff of approximately 16,000 people worldwide

BUSINESS USE CASES

The retail industry faces continual challenges from bad actors which range from cyber attackers attempting to gain access to various systems to counterfeiters selling fake, non-authentic merchandise to unscrupulous competitors trying to disrupt the supply chain. As one of the world's most iconic brands, protecting the company's reputation and its consumers is paramount. For Levi Strauss & Co. this translates into continuous investment in and assessment of cybersecurity programs to reduce ever-evolving risks. Third Party Risk Management (TPRM) is now an essential security component. Organizations across industries must assess third parties for risk to their respective companies. In some industries it is mandated and in others it is just good security practice. For Levi Strauss Inc., it is a key component of the defense-in-depth strategy and is being used to evaluate the security and potential risks the company would be exposed to when opting to do business with a specific contractor, partner, vendor or supplier.

A primary use case is to assess the security posture of contractors, partners, vendors and suppliers to determine the risks to Levi Strauss & Co. and whether to assume those risks. Prior to deciding whether to onboard a third party, it is imperative to be able to thoroughly and quickly assess the security of the third party and the associated exposure.

For bad actors, third parties are often the path of least resistance to compromise or disrupt their end-goal enterprise. As such, TPRM is essential as risks to the third party de facto translate into risks for Levi Strauss & Co. This is increasingly important as third parties are being engaged across departments at Levi Strauss & Co. Therefore, the TPRM solution augmented and customized by the security team is leveraged globally to reduce business risk.

Additionally, as risks continuously evolve, and as Levi Strauss & Co. does not oversee the security programs of its contractors, partners, vendors and suppliers, having a TPRM solution and formalized process that allows for a baseline evaluation followed with continuous and timely assessments of these third parties is vital to on-going risk management.

An added benefit of the TPRM solution is the ability to assess Levi Strauss & Cos.' security program against other consumer facing organizations in the retail space, providing a broader perspective. As TPRM solutions often examine, among other things, publicly available information providing security scores, this enables Levi Strauss & Co. to have a relative gauge to benchmark the company's security program. This not only is useful for the security team but the insight is valued by the executive board.

TECHNOLOGY ACHIEVEMENTS BY IMPLEMENTING TPRM

Through the use of a TPRM solution, Levi Strauss & Co. has been able to add automation, continuous assessment and speed to its third-party risk management program. Employing a TPRM solution provides the capability to achieve much greater insight into third parties, their security posture and potential risks to Levi Strauss & Co. aiding the decision-making process when deciding to onboard a new contractor, partner, vendor or supplier.

BUSINESS GOALS IMPLEMENTING THIRD PARTY RISK MANAGEMENT

Levi Strauss & Co. takes protection of its customers' information seriously and is dedicated to protecting their personal data as if it were it were its own, whether they shop in a retail store or online.

For Levi Strauss & Co. safeguarding the brand and protecting consumer trust is the overarching business goal for implementing a TPRM solution. As a 167-year-old global company with products sold in more than 110 countries and reported net revenues of $5.8 billion in 2019, the value of the brand is immeasurable. Safeguarding the brand means ensuring third parties are as diligent and vigilant regarding security as Levi Strauss & Co., therefore TPRM is of utmost importance.

As such, Levi Strauss & Co. contracts include strict language about what contractors, partners, vendors and suppliers are and are not allowed to do both in terms of security and beyond. Having a TPRM solution allows the security team to monitor third-party compliance with contractual security obligations.

In addition to allowing the business to onboard in a more effective manner to meet business needs, the ability to conduct on-demand security assessments provides continuous visibility into the third party's risk posture and any change in the risk level to Levi Strauss & Co.

Finally, the security team supports business units companywide. When a TPRM assessment is conducted, should the risk associated with a potential partner or supplier be deemed untenable, the security team will advise the partner and if they cannot mitigate the team will work with the internal business unit to select an alternative partner.

KEY FACTORS TO CONSIDER

Managing third-party risk is data reliant. Depending on a company's risk tolerance there are multiple components to a successful TPRM program. For Levi Straus & Co. it was important to have a solution that uses publicly available data and assigns a security score while allowing the security team to augment the data collection with custom questions and incorporate the technology into Levi Strauss and Co's overarching TPRM process. Understanding the methodology and what standards the risk score is based on, as well as the ability to do it expeditiously, were key factors Levi Strauss & Co. considered when selecting a solution.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

A consideration when selecting a TPRM vendor was the total cost of ownership (TCO). Security employees are extremely valuable and have a wide range of responsibilities. It was important for Levi Strauss & Co. to streamline operations as much as feasible to increase turnaround time to onboard contractors, partners, vendors and suppliers without adding additional cycles to the security team and business delays.

A TPRM solution should provide a clearer understanding of a company's cybersecurity posture through risk analysis across multiple security domains. These may include email, governance, and patching among others. It should provide contextualized insight into the risk performance of contractors, partners, vendors and suppliers by continuously discovering their digital footprint and assessing from publicly available sources their risk posture. Various TPRM vendors have different breadth of offerings in terms of the data they access and assess against. Some use recognized standards and others proprietary criteria. Levi Strauss & Co. uses a SaaS based solution that allows continuous assessment.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

Implementing a TPRM solution enables teams across Levi Strauss & Co. to make informed and timely decisions on partners, vendors and suppliers. Once a decision has been made to contract with a third party, the TPRM solution is used to continually assess that third-party to ensure, like with any effective security program, that the level of exposure to Levi Strauss & Co. has not increased.

Additionally, implementing a TPRM solution provides Levi Strauss & Co. data points to use when negotiating cyber insurance policies as often cyber insurance providers themselves leverage TPRM solutions to assess the risk posture of potential insures.

Furthermore, this information, as it provides a quantifiable assessment of the potential exposure to Levi Strauss & Co. in general and as a direct result of contracting with partners, vendors and suppliers, is a valuable component of the annual board meeting as members view this information as business-critical.

STAFFING REQUIREMENTS

TPRM does not add to staffing, to the contrary it allows personnel to better utilize their time as much of the assessment by the solution is done using publicly available information and the team augments it with customized questions based on the third-party, their function and criticality to the business, and the responses are integrated into an overall score and assessment.

PEER RECOMMENDATION AND ADVICE

Understanding and managing the risks of third parties is an essential security component of a company's security program. Whether a business leverages an outside TPRM solution is dependent on their specific needs, business maturity, and budget.

As an early adopter of TPRM technology, it has been a worthwhile investment and is continuing to evolve and provide increasing value. It is important for CISOs to understand the various TPRM solutions available, in particular how they obtain their data, the underlying IP ranges used as the base for a risk score, and against which standards they are providing assessments – are they industry recognized or proprietary standards. As well, the ability of the solution to allow for custom questions impacts the quality of the assessment and score.

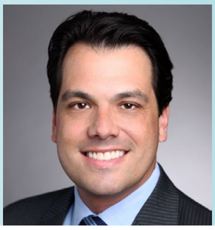
SUMMARY

Third party risk management is a fundamental component of any business security program. Incorporating a TPRM solution into the Levi Strauss & Co. third party risk management process helps to streamline and expedite the decision-making process on whether or not to contract with a vendor, partner or supplier. This provides Levi Strauss & Co. visibility into the security posture of the third party and the potential risk to which the company would subsequently be exposed. As a global brand, for which security is paramount, adding a TPRM solution as part of Levi Strauss & Co's defense in depth program has been a worthwhile investment and something I would recommend my peers consider if they have not yet done so.

HELLMAN & FRIEDMAN PRIVATE EQUITY

MATT HOLLCRAFT

Chief Information Security Officer



COMPANY OVERVIEW

Hellman & Friedman is a global private equity firm with a distinctive investment approach focused on large scale equity investments in high-quality growth businesses. H&F targets outstanding businesses in select sectors including software & technology, financial services, healthcare, retail & consumer, and other business services. Since its founding in 1984, H&F has raised over $50 billion of committed capital, invested in over 90 companies. H&F has offices in San Francisco, New York and London.

BUSINESS USE CASES

Information security within the financial industry, which includes banks, investment firms, and insurance companies, tackles multiple concerns. The obvious role for cyber security is to defend the organization from hackers, attackers, and nation state actors, but it is also an enforcement point for regulatory compliance associated with privacy and managing risks to business operation integrity. Hellman & Friedman's (H&F) cyber security team is well aware of these three components and strives to handle them all.

Third-Party Risk Management (TPRM) helps in shaping the overall security risk mitigation program, but the first priority for a global private equity firm is to conform to a wide range of regulations. You have to adhere to SEC [Securities and Exchange Committee], PCI [Payment Card Industry], GDPR [General Data Protection Regulation] and the California CCPA [California Consumer Privacy Act] as they all have requirements regarding third-party risk.

The need for TPRM isn't limited to internal needs, but also includes those of customers. Third party risk management goes is bi-directional. We require our partners safeguard our data and our partners want to ensure that we secure the data they share with us. As well, we need to ensure that their systems are secure so as not to expose H&F to more risk.

The bottom line is the business cases for third-party risk management are considerable, especially if you have a low risk appetite for any type of loss or exposure of your data.

BUSINESS GOALS IMPLEMENTING THIRD PARTY RISK MANAGEMENT

The first priority for operating a TPRM program should be improving operational efficiency. We are reducing overall risk by having a better understanding of the risk posture of our portfolio companies and other third-party partners, vendors and suppliers. By working collaboratively with other departments within the organization, such as procurement and legal you can increase the level of assurance that the providers can deliver on time, securely, and to the standards to which you agree to in the contract. Efficiency does imply that your partners will not greatly expand your risk, requiring you understand the potential risk and potentially take additional remediation actions.

As a company that is known for its ability to control costs, H&F expects the TRPM program to provide a financial benefit. The method for accomplishing that goal is by lowering your risk profile which saves money on cyber insurance. Demonstrating proper due diligence and best practices you can lower your risk premiums.

KEY FACTORS TO CONSIDER

H&F has an in-house process as well as leverages a TPRM tool which focused on customization. Many products have static workflows, forcing them to put what could be considered a square peg into a round hole. You can't customize completely, but given that every organization is different there needs to be a way to shape the tool to meet your needs. Otherwise you have to modify your processes to adhere to the tool.

Innovation is another key factor. Vendors should be willing and capable of adjusting their product as situations change. TPRM is a laborious and time-intensive workflow, so vendors should concentrate on product improvement. The vendor needs to explain their roadmap for feature and service improvements for six months to a year, or longer if they are planning that far in advance. As well, it is optimal when selecting a TPRM tool to know against which standards it is scoring vendors. Is it a recognized standard or is it something they have developed?

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

A common challenge is lack of conformity in reporting. Any business report, audit report, or regulatory finding may have a similar meaning or context. Because they are composed differently, they do not look the same, making interpreting the data difficult.

AI [Artificial Intelligence], or more precisely Machine Learning capabilities, can perform natural language processing. This system should be able to review a collection of security reports looking for keywords and determine at what level the two are similar. To the human eye, a number of reports may look completely different, but to the machine they are essentially the same.

There also is a need for TPRM systems to share and collect information from public databases. Documents produced to provide information on security capabilities should be shared across different third-party risk management systems. The products should also be able to connect with public databases that would have useful data, such as 10-K filings.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

H&F encourages all company organizations to work together when performing third-party risk assessments. A platform solution can allow for the integration of the product and service procurement process, allowing risk to be considered during the purchase process. Security and risk management should be part of the decision-making beforehand, otherwise you might be required to bolt on a security or risk mitigation fix after-the-fact.

TPRM platforms should also offer the ability to incorporate all stakeholders, by allowing them to sign-off on the risk directly in the product. The person who's buying the product or service is the primary risk holder, but of course legal and cybersecurity own some portion of that risk. Especially if they are going to be connecting to, processing data, or connecting to the network. Documentation needs to be searchable and recoverable as part of this workflow.

IMPACT ON STAFFING LEVELS

Plan on increasing staff to meet the growing demand for third-party risk assessments. Many firms, especially in the financial and healthcare sectors have already done so. As technology improves, especially with better data management and more natural language processing, automation will serve in these roles.

PEER RECOMMENDATION AND ADVICE

TRPM is not as easy as it looks. You quickly discover there are more components than initially expected, because more stakeholders are involved and impact the decision-making. You should avoid complicating the process with slow or impeding business operations. A criticism of cybersecurity is it strives for perfection instead of shooting for the best possible outcome.

For the industry overall, there should be more collaboration among industry sectors, especially regarding the sharing of information. Nine technology companies founded the Vendor Security Alliance [www.vendorsecurityalliance.org] which is an independent, non-profit coalition that aims to help member companies evaluate or assess the security and privacy of third-party providers whom they heavily rely on safeguard important user data The coalition has taken upon itself to create a benchmark of acceptable cybersecurity practices vendors need to comply with.

SUMMARY

The primary role for cyber security is to defend the organization, while adhering to regulations associated with privacy.

It is expected that the capabilities of TPRM products will evolve and expand. Future improvements could include improved AI for natural language processing, and for systems to improve collaboration through the standardization of reporting and the sharing of information.

H.I.G CAPITAL

MARCOS MARRERO

Chief Information Security Officer

COMPANY OVERVIEW

H.I.G. Capital is a leading global private equity investment firm with $37 billion of equity capital under management. They provide both debt and equity capital to small and mid-sized companies. The company's 350 investment professionals align themselves with committed management teams and entrepreneurs and help build businesses of significant value. H.I.G. Capital is headquartered in Miami with offices located throughout the United States, Europe, and Latin America.

BUSINESS USE CASES

For H.I.G. Capital security is paramount and as a leader in the finance industry, which is a prime target for hackers, we maintain a dynamic and robust information security operation. A key control to ensure the security of our systems and data is our third-party risk management (TPRM) program. As a private equity investment firm with billions of dollars under management it is imperative for us to have a complete view of our risks whether they are direct or via a relationship with a vendor, supplier or partner. We must understand the risks we decide to assume, as there are always risks, when we enter into a new relationship and as the relationship continues.

As part of our process we leverage a TPRM vendor to assist us in our analysis of the security posture and controls when onboarding a new vendor, supplier or partner to determine the robustness of their program and our associated security risk and potential exposure. This information is avkey element in deciding if we enter into a business agreement. In addition to leveraging our third-party tool for onboarding we continue to review and perform these assessments on a regular basis, either quarterly, semi-annually, or annually depending on the level of criticality we assign to the vendor.

At H.I.G. Capital our business units, of which technology and security are key components, work closely together. As the Chief Information Security Officer (CISO), my team assesses the risk and potential ramifications and provides our determinations to business operations which then decides if it is a risk the business is willing to incur. During our assessments by and large we find that the vendors are employing appropriate security controls but on rare occasions based on our findings we make a conditional approval which requires the third party to close a potential security gap if they want to move forward with us. Should we determine that security is not paramount to a third party and/or they have blatantly failed to implement basic security controls we could offer up a flat-out denial but as of yet we have not encountered that situation.

BUSINESS GOALS IMPLEMENTING THIRD PARTY RISK MANAGEMENT

The process of conducting TPRM assessments can be an excruciatingly time consuming process. At H.I.G Capital one of our key goals around using a TPRM solution has been to reduce the time required for each assessment, thus increasing the productivity of our employees. By streamlining and integrating the tool into our processes we can conduct quality assessments as quickly as possible. A TRPM solution should improve automation which fosters the development of a comprehensive assessment in days to week, down from what we found had been a week to a month or more. As well, process improvements, especially in the area of communications and document sharing with our potential and existing third parties, should enable them to collect, generate, and share with us the information required for the assessment. Based on our specific needs, as each organization has considerations, having a tool that scores the party's risk in a quick and easy way maintains ongoing assessments and alerts us if anything has changed.

It is encouraging that TPRM solutions are improving and gauging their assessments against recognized standards such as the NIST Cybersecurity Framework. This helps not only ensure compliance but gives us additional confidence while removing us from the day to day data collection and processing. We are still highly involved in assessing the risk of our suppliers but we do this in tandem with an outsourced solution. Using a service that performs TPRM data collection on a large number of companies helps us fast-track the assessments, getting them done in a much quicker and effective manner, helping the business onboard suppliers to move operations forward when necessary.

KEY FACTORS TO CONSIDER

At H.I.G. Capital, we have identified top consideration to be the ability to continuously monitor a third party's risk profile and to be able to assess that risk relative to previous assessments. By doing this the TPRM vendor seamlessly finds the deltas between the latest review and previous assessments. This allows us to require additional action only on those new potential risks.

As well, it is important that if opting for a TRPM solution that it is grounded and carries out its assessments against recognized standards. We have found that this provides peace of mind and in addition to helping assess the risk to the business, aids us in our compliance mandates as well.

Regarding reporting capabilities, we prefer an easy to consume solution that allows us to quickly see the security posture of the vendor and draw attention to any substantive changes or red flags. For us, having assessments reported using a green, yellow, and red scale with green being approved, yellow being conditionally approved and these are the conditions or gaps we still see, and then red being a recommendation to not approve is most effective. Even with that scale, we still ensure we have the ability to adjust the results by having the system take into consideration changes that relate our analysis of the data which we base on our specific needs and level of risk tolerance.

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

Ironically, when I think about the technology components I'm looking for, I concentrate on those solutions, whether it is TPRM or some other operation, where I don't have to worry about the technology. For our company it makes sense for someone else to operate the servers and the back-end infrastructure. At H.I.G. Capital our solution is an easy to use SaaS portal that can be utilized by other entities within our organization. This capability allows for all relevant staff, whether it is legal or business operations, to use the portal to request or execute new reviews, to track the progress of the review in real time, monitor document status and submissions, review the data of value to them, and generate a final report on the vendor risk assessment to make informed decisions.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

Onboarding vendors, suppliers and partners has become much easier and less time consuming since adopting a TPRM solution. By having a platform that has a lot of the information already available we can conduct more assessments in shorter periods of time and the continuous review process once a third party is onboarded is much easier too. Using a TPRM solution where information associated with previous assessments is already available and evaluated against provides quick and greater context. This allows us to focus on the information, analyze it, and decide if steps need to be taken. In the end, it reduces all of the back and forth associated with assessments and data requests.

IMPACT ON STAFFING LEVELS

At H.I.G. Capital we have one person who oversees TPRM assessments. It's not their full-time job, but it's part of their scope from a governance, risk and compliance (GRC) perspective, which is where the vendor risk assessments fall in our information security program. That person splits their time between doing the vendor risk assessments and other GRC tasks. The TRPM tool alleviates some of the time-consuming activities which allows my analyst to better utilize the time allocated to TPRM by augmenting it with more or more in-depth evaluations.

The process improvements associated with a TPRM solution should assist larger organizations as well. We have found that having a TPRM solution help expand our overall security and risk analysis capabilities and knowledge.

PEER RECOMMENDATION AND ADVICE

My one recommendation is that regardless of the type of solution you are looking for be it SaaS-based or on-premises or outsourced, you must conduct a proof of concept test. Companies will tell you, "Hey, we can run all these assessments for you. We've got data on all these organizations. We have access to all their SOC 2 reports or SOC 1 reports and controls documents." Don't take their word for it but have them run a few assessments on some major technology players and maybe some of the smaller vendors you utilize so that you can get actual output so you can determine if it meets your needs. As part of your due diligence reach to our CISO peers who have first-hand experience and can provide real-world feedback, including but not limited to the TPRM solution provider's responsiveness.

SUMMARY

Hackers are constantly on the hunt, looking for juicy targets that they can sink their teeth into. They are looking for things to sell and financial data is lucrative. H.I.G Capital is serious about protecting our customers and clients but to accomplish this task it is important for us to understand what security risks we assume when we enter into a relationship with a vendor, supplier or partner. We have a TPRM solution and process which allows us to analyze the security controls that an outside third party has in place to determine its effectiveness.

All organizations should be concerned about their third-party suppliers but the process of conducting TPRM assessments can be a painful and time consuming. To reduce the time and effort required for each assessment the endeavor needs to be streamlined. There must be improvements in the areas of information reuse, document sharing, and communications. Those elements are where your TPRM vendor should have proven expertise.

NEXTEER AUTOMOTIVE

ARUN DESOUZA

Chief Information Security & Privacy Officer

COMPANY OVERVIEW

Nexteer Automotive – a global leader in intuitive motion control – is a multibillion-dollar global steering and driveline business delivering electric and hydraulic power steering systems, steering columns and driveline systems, as well as ADAS and automated driving enabling technologies for OEMs around the world.

Nexteer has more than 110 years of automotive experience, and today, we serve more than 60 customers in every major region of the world. Our global workforce of more than 13,000 is a rich tapestry of people of diverse cultures filled with a collaborative spirit and passion for relentless innovation.

BUSINESS USE CASES

Global businesses in the automotive industry face varied challenges from international compliance mandates, to cyber attackers trying to gain access, to ensuring the uninterrupted flow of the supply chain. As a company with an international workforce serving customers worldwide, protecting Nexteer's ability to conduct business while safeguarding its reputation is business critical. For Nexteer that means creating holistic, multi-dimensional layered security programs that focus on people, processes, and when required, technology. Regardless of industry, Third Party Risk Management (TPRM) is a key component of a successful security program and instrumental to ensure the continued growth and success of our business.

As the CISO it was vitally important at the start of my tenure five years ago to build an overarching security and risk framework to facilitate the exchange of information across a far-flung employee and customer base. As is common in the automotive industry we based it on the International Standards Organization (ISO) model.

ISO is the foundation of Nexteer's TPRM program, which continues to evolve with changing demands, including compliance, in particular the European Union's General Data Protection Regulation (GDPR), which was the catalyst for the comprehensive risk management process now in place. As GDPR regulates the exchanges of personal data for business purposes between the European Union and the United States, being in breach of the GDPR could not only lead to massive financial penalties but leave Nexteer vulnerable to civil lawsuits.

I pioneered a holistic information security and privacy program. I envision that the enterprise is moving towards a convergence of the security, privacy and enterprise risk functions.

At Nexteer, as CISO I am responsible for security and privacy while working closely with the enterprise risk group. The security team also works across the enterprise and the processes in place are driven by the various business units. The associated steps within the TPRM program are directly related to the particular function of the third party in scope and the risk to which they expose Nexteer.

BUSINESS GOALS IMPLEMENTING THIRD PARTY RISK MANAGEMENT

There are various business goals driving the company's TPRM program which is built in house and continues to evolve. Compliance was the initial impetus of the program to ensure that Nexteer, which conducts business in the EU amongst other countries, met GDPR mandates to avoid penalties and civil lawsuits. As compliance is just one piece of the security, privacy and risk puzzle, the TPRM program has grown to represent the natural convergence of the responsibilities.

At a strategic level we strive to consolidate security, privacy and risk into a unified approach to TPRM as the risk potentially introduced by a third party directly impacts security and privacy across the business. This is key on a day-to-day operational as well as a long-term strategic business basis. The process to onboard and leverage third party partners, vendors and suppliers, has the potential to either facilitate or if done inappropriately hinder the company's growth.

Importantly, the risk posture of the third parties that Nexteer contracts with directly impacts the risk posture of the company and hence is just sound business practice to have a robust and proactive process in place that allows for onboarding and continuous assessment of the third parties.

KEY FACTORS TO CONSIDER

As Nexteer continues to mature its third-party risk management it is important to create repeatable processes within a structured format. Ideally this could be enacted by a technology platform that is driven by the business and incorporates People, Process and Technology. It is essential that whether it is built in house or in conjunction with a third-party tool, the platform or solution provides metrics on the health of the program within an easily understandable format. In our case that is in the form of a scorecard generated by a questionnaire that we created and we provide to our third parties. Once a platform is deployed, it could be input into the platform and enable leveraging supplier analytics which would enable visualization of risk and compliance across our partner, vendor and supplier ecosystem.

It is imperative to stack rank major suppliers and to drill down further to manage risk, which can take various forms and eventually could directly impact, if disrupted, Nexteer's ability to service its global customer base. In that sense, when examining risk, it may be -- depending on the third party and their importance and function -- business critical to check the financial health and their stability as well as their security posture. To ensure the efficacy of these activities, so that Nexteer is safeguarded across the business, it is important to build cross functional coalitions especially with purchasing, legal and enterprise risk. By pulling together these cross functional views, stakeholders are able to gain visibility, and make better decisions.

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

A central technology component is a vendor inventory or repository where third-party information, including the completed questionnaires, open source data, and internal assessments are stored and accessed. Other key technology components are the ability to process the workflow and foster the sharing of information.

The desired goal is to make the TPRM process more efficient, by leveraging a cloud-based platform that contains an extensive database of vendor information that performs many of the simple tasks using automation and orchestration. To leverage the platform an enterprise asset, it has to enable self-service and have a common user interface so that anyone from legal, procurement, IT, security, and executive management can interact with the system to populate it with data, gain additional knowledge, and record decisions.

IMPACT ON STAFFING LEVELS

At Nexteer, we leverage our existing personnel within security, privacy and risk while conferring with legal and procurement among other business areas of the organization to effectively manage our third-party risk.

Ideally, depending on the maturity of an organization and available budget, to stay ahead of the curve, the creation of a central risk organization that would oversee from a holistic perspective risks introduced by third parties would be most effective. This consolidated function, ideally a Project Management Office (PMO) within the risk organization, would enable the business to measure and report risk, and would initially require a program manager, director and one to two analysts.

PEER RECOMMENDATION AND ADVICE

As CISOs are key executives within the organization, I would recommend viewing third party risk management as a cross functional endeavor. Increasingly there has been a convergence of security, privacy and risk of which I am proponent as it leads to a more effective and holistic approach. Engaging security, technology, legal, procurement, senior management and among other personnel ensures third party risk is assessed on a continuous basis against potential business impacts be they from a potential breach to a disruption of the supply chain.

TPRM should be looked at from a people, process and technology perspective. I would recommend, depending on the maturity and budget of the organization, creating a PMO specifically to oversee third-party risk. Regardless, to be successful it is critical to build cross functional coalitions within your organization and provide easy access to easily consumable assessments. In our case that is enacted in the form of a scorecard, to allow technical and non-technical personal across the organization to utilize and contribute to the information to make better decisions.

SUMMARY

TPRM is a necessary component of any security organization whether it is to safeguard against bad actors, protect the supply chain, maintain compliance or protect the reputation or brand of a business. Ideally, a PMO office overseeing risk based on security, privacy and compliance would be the standard.

As security, privacy and risk operations continue to converge, it is advantageous to work across roles within an organization and create cross functional coalitions. Having a program that is platform based with easily consumable information that empowers stakeholders to make informed decisions will help grow the business while continuing to protect it.

PREMISE HEALTH

JOEY JOHNSON
Chief Information Security Officer

COMPANY OVERVIEW

Premise Health is the world's leading direct healthcare company. The 50-year-old company headquartered in Brentwood Tennessee provides onsite and near site health centers, and 24/7 virtual health. Premise offers 26 different products and customizable services, has built and managed over 600 wellness centers in46 states, making them the nation's largest direct access care network.

Premise Health uses advanced technology to create a first-rate experience before, during, and after care.

BUSINESS USE CASES

Premise Health is committed to our members' privacy and security. We are certified under the HITRUST Common Security Framework, meeting the strict healthcare regulations and requirements for protecting and securing sensitive private healthcare information. Additionally, Premise Health is subject to hundreds of client risk assessments annually, providing us perspective on both the issuing and receiving sides of third-party risk management operations and outcomes.

Third Party Risk Management (TPRM) is key to our overall risk strategy, and is tightly aligned with our Legal, Procurement, and Growth functions. The tools we opt to leverage need to augment our overall vendor management program to enable us to collect and consolidate a complete picture of vendor risk levels, and how they change over time.

Looking at TPRM from the narrow scope of IT security, the program provides tangible risk reduction by identifying partners of concern. We are able to decide partner engagement based on these risk levels, or to help them mitigate the risks uncovered as part of the evaluation. In a manner that may seem counter-intuitive, we often leverage the TPRM program as a means to rapidly mature an immature partner to facilitate faster speed to market with certain service offerings.

BUSINESS GOALS IMPLEMENTING THIRD PARTY RISK MANAGEMENT

The first goal of a TPRM program is to reduce the overall business risk to the organization. Medical information is a prime target of adversaries and regulators and our client base keep a close eye on how we protect Personally Identifiable Information (PII) and Protect Healthcare Information (PHI).

A primary business goal is to have a holistic view of our third-party relationships. The first task is to create a complete inventory of the vendors, determine how vital the business of those vendors is, what type of information is shared, and the sensitivity of the data. The visibility into the vendor landscape through TPRM activity facilitates better internal business connections and helps to position Security as a critically integrated business function.

KEY FACTORS TO CONSIDER

When considering how to structure your TPRM program, you can develop your own solution or use an outsourced product(s) and/or services, or implement a combination of both. An in-house solution places key activities into the hands of staff, while many outsource the often mundane and repetitive tasks. It boils down to what is best for your organization.

Premise Health outsources much of the basic functions, especially collection and review of large volumes of data artifacts. We decided there were many value-added activities our experienced staff could be performing as opposed to reviewing documentation.

There is a myriad of documents - policy and procedure documents, SOC reports, penetration testing reports, questionnaires, audit reports, HIPAA reports, etc. All of these documents need to be tracked, shared, reviewed, searched, retrieved, and archived. Any system you develop or purchase must have a robust document handling system, and part of that system is to ensure those documents stay secure.

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

Third party risk management is a human centric activity, but technology makes the process much more efficient. TPRM has been a process for Premise Health for many years, and multiple product evaluations have made a number of technology components stand out as critical. First and foremost, a cloud platform has proven efficient given all of the documents needed to be exchanged between third parties.

Contacts outside of the third-party risk management program need access to our documentation, artifacts, and data. An accessible web portal is needed for login, and the TPRM platform requires a mechanism to communicate via email and the platform.

The most critical TRPM portal feature is auditability. Understandably, vendors are concerned about the sensitive documentation they are submitting. With so many sensitive documents residing on the platform, it's important to clear audit trails which identify who logs into the platform, views, accesses, modifies, and deletes files.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

Premise Health has reviewed the risk associated with third-party vendors for a decade. The experience has been extremely valuable to the organization from both a business and cyber security standpoint. We have reduced the overall risk to the business, however, it has been a long and interesting journey.

When the effort began, we quickly determined which vendor relationships we wanted to retain. We discovered many of the companies were not working under contracts, but were hired by different business groups. Contracts are the primary linchpin by which you establish security rights and liability for the organization. Procurement and operations conducted a deep review of suppliers and found considerable duplication and overlap. As a result, we reduced our vendor population significantly.

Our TPRM effort is our security program tied most closely to the business units, resulting in our security mission becoming wholly engaged in business operations end-to-end. The program drove exposure to security as a primary core business function as opposed to being a siloed technical function. Security is now a visibility point for the organization, as many different parts of the company come to security for advice regarding risk. Careful deliberation with company stakeholders, and sometimes vendors, would provide alternatives or modifications to mitigate risk.

The TPRM efforts also uncovered when some operatives within the organization were outside of our risk tolerance level. These operatives were working at higher levels of risk acceptance without necessarily being authorized to make those kinds of decisions.

IMPACT ON STAFFING LEVELS

Premise Health increased TPRM staff, but it was a gradual process. Initially, the IT security staff was small and one-point person would speak to our legal and procurement teams regarding contract reviews from a third-party risk perspective. As CISO, I also was responsible for responding to our clients who sent us questionnaires. It quickly became clear the level of effort required additional staff.

The TPRM program grew as Premise Health stakeholders recognized the value of having security involved in the vetting of vendors. First, the governance manager was enlisted to participate and eventually a staffer was hired to work exclusively to handle TPRM activities. The number of employees covering third party activities has continued to grow with added value to the program.

PEER RECOMMENDATION AND ADVICE

TPRM should be a process to help vendor partners achieve maturity, especially those small and medium sized partners. The TPRM process shouldn't be a simple measurement activity, but instead should ensure the business units are able to work with the best solutions available. Using guerrilla tactics where you can help the partner reach a mature and acceptable level of security is the business Premise Health really wants, creating a competitive advantage.

There is an opportunity to flip the TPRM processes from a pure evaluation into a consultative activity, developing relationships, building partnerships, and tangibly reducing risk. Frequently Premise Health partners and vendors start out insufficient from a security perspective to meet the high bar requirements that Premise Health demands. In those cases, sending them a long questionnaire simply results in long timelines for completion to ultimately find out what you already knew going in. Rather, propose to help improve their security position. You can conduct a penetration test or lend them a security engineer for a day to help them stand-up a needed security product. By assisting the third party in this manner, you have a much better appreciation of, and visibility into, their technology footprint and what their risk is without having to go through four months of back and forth questionnaires.

Bottom line, working as an advisor delivers real value to the business. Additionally, it creates an environment of trust where the partner is willing to be transparent with risk scenarios and how to best mitigate them, rather than one in which risk scenarios are concealed for fear of losing the business relationship.

SUMMARY

TPRM has been extremely valuable to the organization from both a business and cyber security standpoint. Developing a mature third-party management process takes considerable time. The process is key to our overall risk strategy, in that it provides a comprehensive picture of vendor risk.

RICOH USA, INC.

DAVID LEVINE

Vice President of Corporate and Information Security, CSO

COMPANY OVERVIEW

Ricoh empowers digital workplaces using innovative technologies and services, enabling individuals to work smarter. For more than 80 years, Ricoh has driven innovation and is a leading provider of document management solutions, IT services, communication services, commercial and industrial printing, digital cameras, and industrial systems.

Headquartered in Tokyo, Ricoh Group operates in approximately 200 countries and regions. In the financial year ended March 2020, Ricoh Group had worldwide sales of $18.5 billion.

BUSINESS USE CASES

Ricoh USA, Inc. supports consumers and companies of all sizes. As security is of utmost important to Ricoh, it is business critical that we have confidence in the security programs of our third-party vendors, partners and suppliers. To ensure this, we have established polices and procedures, including how to assess and evaluate the risk to which a third party potentially exposes Ricoh. A key part of the process is an in-house security questionnaire that allows us to determine the risks associated with potential third parties we may engage with and also use it on an as needed and or recurring basses to re-evaluate risk.

In order to accurately assess the potential risk to Ricoh, our questionnaire covers a wide array of domains, goes beyond simply yes and no responses, allows the partner to provide context for their answers as well as documents the data involved. We also frequently provide the opportunity to potentially allow a prospective partner to mitigate a potential risk to meet our security standards.

In some cases, we augment our questionnaire with a third-party risk management/scoring solution and we have a business unit that just started utilizing a SaaS based Third Party Risk Management (TPRM) Platform.

BUSINESS GOALS IMPLEMENTING THIRD PARTY RISK MANAGEMENT

Successful cybersecurity, and in particular TPRM, requires a program guided by policy with clear and consistent processes. At Ricoh, the business goal is to protect our data, reputation and supply chain. Leveraging a formal TPRM tool in the future, in addition to our in-house questionnaire, will provide us with a variety of important benefits including; an automated way to record and notify when follow-up or vendor re-evaluations are required, scheduling, cataloging, maintaining a single repository of our third-party risk documentation, and supporting compliance requirements. Depending on the platform, you may also be able to leverage it to provide important information when responding to questionnaires from your third parties.

KEY FACTORS TO CONSIDER

There are several factors that need to be considered, most importantly being your particular goals. Are you looking to automate processes, which may include, for example, report generation, automated notifications, and responding to and sending questionnaires? Just looking for a repository? Both? Depending on the answer, you may want to assess whether there is a tool that meets your needs or is an in-house option preferable.

Evaluating the security of the solution itself needs to be considered. You are placing a great deal of critical information about your security and governance programs as well as the answers to partner risk assessment questionnaires into the tool. Trusting that this information is safeguarded is required.

Flexibility and ease of use within a tool is also a key factor. Examples in this area include: being able to use the platform for both internal and external questionnaires; customizable reporting, presenting questions and information based off of specific needs or based off evaluating specific solutions, allowing for more than just simple yes and no answers (context matters) and the solution should be easy to navigate.

An appropriate workflow is also necessary, keeping track of all TPRM assessments and providing automated reminders for required actions is basic but key functionality and the workflow should be able to be tailored to your needs and not need to rely on a generic process created by the vendor.

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

Like all SaaS/Cloud based solution you don't have to worry as much about maintaining the infrastructure; however, as noted above, you should evaluate a potential TPRM solution just like you would any platform that will hold confidential and detailed information. Security controls and governance matter just as much here. Is the data encrypted? Does it support MFA? How is the data backed up? Who has access to it, etc.?

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

Adding a dedicated tool, various components, or platform will aid you in performing required TPRM tasks and should improve the efficiency of the overall program, offer easy access to data, support your governance requirements, and streamline collection and dissemination.

IMPACT ON STAFFING LEVELS

Depending on your staffing levels, the efficiencies gained by using a TPRM tool may either free up time and resources, or could result in more assessments being done as you mature the process and thus there may be a need to justify additional staff.

PEER RECOMMENDATION AND ADVICE

Beyond the tool and processes themselves, what really needs to be addressed is standardization. We all need to be able to asses the security and risk of our third+ parties but today we do it in disjointed, unproductive, overly burdensome, time consuming and in many cases misleading ways. Having a common framework, set of frameworks or standard regarding the information required would ease the burden we all face in performing third-party risk evaluations.

The questions asked of third parties also need to be useful and germane. Questions that only allow YES/NO answers do not convey the depth of information required for proper decision-making and applicability matters. As noted, the significant variation of surveys and details required creates inconsistency in the space.

SUMMARY

A successful TPRM program addresses the need to assess the risk of vendors, suppliers and partners. It should be efficient, relevant to the data and solutions in scope and should also provide an open conduit for security peers to discuss questions when and if needed. Ultimately, we need a better and more consistent way to conduct assessments.

RWJBARNABAS HEALTH

HUSSEIN SYED

Chief Information Security Officer

COMPANY OVERVIEW

RWJBarnabas (RWJBH) Health is the most comprehensive health care delivery system in New Jersey, treating over 3 million patients a year. The health system is New Jersey's second largest employer – with more than 32,000 employees, 9,000 physicians and 1,000 residents and interns, and 240 medical practices. The system includes 16 hospitals, 5,000 beds, acute care facilities, ambulatory care centers, comprehensive home care and hospice programs, fitness and wellness centers. RWJBarnabas Health was created through the 2015 merger of the Robert Wood Johnson Health System and the Saint Barnabas Health Care System.

RWJBH provides patients a full array of services, including emergency medicine and specialty services such as heart transplant or renal transplant. The health system ranks #2 overall in renal transplant services, and is the largest provider of renal transplants involving live donors.

RWJBH does over $5 billion in revenue a year, based on reimbursements.

BUSINESS USE CASES

Healthcare organizations are obligated to protect private personal information under the Health Insurance Portability and Accountability Act (HIPAA). However, meeting that requirement can be difficult as healthcare providers as part of servicing their members share patient information with many partners, including labs and insurance companies. Further complicating the issue, healthcare records are extremely valuable to hackers, selling on the Dark Web for 10 to 40 times more than credit card numbers. One dark web post advertised an entire hospital database totaling 397,000 medical records.

This backdrop is critical in our need to understand the security posture of suppliers providing outsourced services, doing offsite data processing, or granting a third-party direct access to your network. Conducting third party risk assessments on your supply chain partners meets a number of needs covering regulatory compliance, cyber risk management, intellectual property protection, and business continuity.

THIRD PARTY RISK MANAGEMENT BUSINESS GOAL

RWJBH outsources some activities, which may include sharing patient data. As the privacy of our patients and staff is paramount so is our security to ensure that. In order to do this, we need to ensure that any information provided to those suppliers does not adversely impact the overall risk profile or expose personally identifiable information (PII). RWJBH has an extensive third-party risk management program and the information security department is responsible for evaluating the security risk associated with those third parties. The security team provides an impartial risk assessment report to the business unit manager, who is requesting the outsourcing service. They can make an informed decision on whether or not to engage with that third party.

The evaluation summarizes which risks adhere with policy and which do not. Security coordinates with the legal department to develop and incorporate any language or stipulations that should be added to the contract. It's becoming common to consult legal departments to see how liability indemnifications and requirements associated with cyber insurance are affected by third party arrangements, especially for those hosting data or performing a critical business function.

KEY FACTORS TO CONSIDER

Given the wide range of material associated with vendor risk management and the rapidly changing nature of security threats, we determined that in addition to our in-house third-party controls we wanted to leverage a third-party tool to augment our processes. That solution had to be flexible, agile, and nimble enough to incorporate changes to the process or overall situation.

In addition to adaptability, the solution had to offer significant automation and avoid repetition. Handling long-term relationships with providers requires frequent document updates and changes to risk reports and assessments. The system had to foster the ability to retrieve the reports, pull in outside data from other tools, and reduce the number of manual tasks associated with reporting and managing the TRPM program.

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

We selected a SaaS solution because it frees us from the issues of building and maintaining the servers, software, and networking components. We found that using the cloud fit our need in handling all of the documentation required to conduct assessments. The solution is able to handle our document workflow.

One key technology related to the SaaS platform that we required was strong authentication and authorization. When we are engaging with our vendor, we set a profile up and send them an invitation to log into the solution. From there they can update their information, attach documents, and interact with our risk assessment team.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

Adopting a TPRM solution has improved our time management. Our internal goal is to complete each thorough risk assessment in three to four weeks. Achieving this goal is one of the quantitative measures on the success of our solution.

The tool we selected makes modifications and updates easier, managing the complete life cycle for our third-party relationships. From a security perspective, we would like to be notified if there are any changes to the external security posture as reported by security rating services. Additionally, the security team continues to remain work with RWJBH business leaders in order to update or reassess our vendors should the business requirements change.

Our TPRM creates a record of security technical controls used by our partners. Armed with this information, along with our internal security assessment, there is enough material to help gauge the overall risk of data exposure. With this information, cyber security insurance companies can offer us appropriate rates and the proper level of cyber liability coverage.

IMPACT ON STAFFING LEVELS

With automation, such as the ability to scan answered questionnaires and determine which are answered with a minimum threshold, an assessor only needs to directly review those areas of concern. This process moves the workflow along.

As TPRM processes mature, the equation regarding staffing may change and potentially increase. Companies will expand their operations, requiring more resources such as people, tool-based automation, or a combination of both.

PEER RECOMMENDATION AND ADVICE

The greatest difficulty associated with TRPM, especially if you are establishing a program for the first time, is you have no real idea what you are up against until you delve into the issue. Once you get into third-party risk, you start uncovering business operations and discover many business functions are handled by or with third parties. Some relationships might not be well documented because they are built upon long term relationships.

It is only when the CISO becomes part of the business engagement process that many of the existing third-party relationships are evaluated from a security risk perspective. This insight can facilitate communications with the business leaders on the value of risk management, especially as it pertains to third parties, and provide the assistance they require in addressing any risk issues.

CISOs should evaluate TPRM tools based on their ability to incorporate a holistic approach covering business requirements, regulatory components, and understand the cyber liabilities facing the organization.

SUMMARY

The healthcare industry is highly regulated, especially when it comes to the protection of PII which is a primary target of hackers. Healthcare providers also outsource a number of activities which require the sharing of information. Establishing a Third-Party Risk Management process helps ensure shared and regulated PII is safeguarded. Using a TPRM system allows the security team to provide an impartial risk assessment which provides insight as to the potential risk enabling business leaders to make decisions regarding suppliers. Additionally, the TPRM solution creates a record of security technical controls used by our partners. Armed with this information, along with our internal security assessment there is enough material to help gauge the overall risk of data exposure to make informed decisions.

SERVICEMAX

AL GHOUS

Chief Security Officer

COMPANY OVERVIEW

ServiceMax is the global leader in Service Execution Management, a software category that includes both Field Service Management and Asset Service Management. ServiceMax provides a cloud-based software platform that improves the productivity of complex, equipment-centric service execution for OEMs, operators, and 3rd-party service providers. Enterprise companies across the globe have turned to ServiceMax to transform their service from a reactive break-fix model to a predictive service that minimizes unplanned downtime. ServiceMax processes more than two million work orders every month, created by more than 350,000 technicians around the world, servicing more than 200 million units of equipment.

BUSINESS USE CASES

ServiceMax is a cloud-born company still operating in the cloud. Customers, mostly large enterprises, rely on the company's software platform to provide critical services to their clients. These customers provide lifecycle management and maintenance support of devices and equipment they manufacture, preventing the support personnel from accessing the ServiceMax cloud-based platform. Contractual repair and up-time service would damage the customer, and could cascade down to their user.

It is critical to understand partner security hygiene to identify any potential risk and make informed decisions around further engagements. In particular, it is important for us to monitor the risk associated with the third parties that directly impact our product functioning. Issues translate into a supply chain management dilemma, as ServiceMax is directly impacted and accountable for the third and fourth parties.

Third Party Risk Management (TPRM) is about ensuring partners do not introduce unnecessary risk that could impact the reputation as a trusted security partner. We believe TPRM allows us to facilitate client assessments and communicate our security posture to customers in exchange.

BUSINESS GOAL IMPLEMENTING THIRD PARTY RISK MANAGEMENT

As a company dependent upon other suppliers, it is critical for ServiceMax to have of that our third parties are reliable and low-risk. Through TPRM, we have a central risk management point to navigate where risk is most acute.

One TPRM goal is to proactively provide our current and potential customer base transparent information about our security posture to illustrate our reliability. Our TPRM platform is leveraged to be an intermediary between us and our customers, where we can create a cloud-based profile with fundamental elements, such as self-assessments or certifications. Ultimately, when systems are advanced enough to allow the re-use of assessment data, we expect a modern TPRM cloud-based platform to reduce the need to answer detailed questionnaires and attend multiple meetings.

The final business purpose of our program is to satisfy auditor requirements.

KEY FACTORS TO CONSIDER

As a provider of cloud services, we embrace using a cloud-based software-as-a-service (SaaS) TPRM platform. SaaS lowers overhead and increases the ability to scale as the TPRM program grows.

Risk assessments are difficult to perform, especially when third parties are involved. A key consideration for ServiceMax is having the ability to automate the creation, collection, sharing, and analysis of multiple assessments simultaneously. The tool should also be flexible enough to accommodate our risk assessment approach and risk management practices. It should allow for continuous assessment throughout the year in addition to the initial assessment which is conducted to determine whether or not to engage the third party.

An automation of threat information and general news also helps us stay ahead of any issues, and respond in a more-timely manner. Notifications surrounding an attack or breach to our ecosystem is also beneficial.

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

Third-party risk management activities are best handled as a web service, due to the involvement of multiple parties. Companies need to share data. Therefore, a cloud platform is best suited as the repository for storing, sharing, and updating the required information. The platform should allow for the automation of mundane redundant tasks such as email notifications, strong search capabilities, and the ability to generate real-time dashboards.

A key technology that all TPRM systems should have is the ability to leverage APIs (Application Programming Interfaces). Opening up APIs facilitates integration with other third-party tools like ticketing systems, bug tracking systems, risk assessment tools, directory services, single sign-on and other functions.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTIONS

For ServiceMax, the ultimate outcome is the ability to wrap our arms around third-party risk. Using an agile, flexible, and modular platform we will have a tool to understand our third-party risk and make informed decisions based on the analysis of the data. We expect to achieve a complete view of all our third-party risks in near real-time, and be able to use a dashboard to disseminate the appropriate information to our business units.

Affordability, by using a SaaS platform, allows us to budget operating expenses, not capital expenses. The capital budget remains available for business operations.

IMPACT ON STAFFING LEVELS

Purchasing any tool should be done to augment activities performed by the staff. TPRM is no different. Security analysts or engineers involved with TPRM can be freed from many of the mundane tasks, such as sending emails, setting up meetings, database entry, assessing the completeness of questionnaires, and calculating a risk score. All of those tasks should be automated using the tool.

PEER RECOMMENDATION AND ADVICE

TPRM should always keep up with technology. Focus on other product offerings, new technologies being developed, and vendor road maps. If you already have a tool and are not happy with it - don't be complacent. Look elsewhere for a new provider that allows you to take advantage of new developments in data management, automation, and APIs. Disruptive vendors can help facilitate exporting your data from your existing system to the new platform.

SUMMARY

For ServiceMax, third-party risk management flows in both directions. We perform third-party assessments on our suppliers and we are asked by our customers to demonstrate our security posture. Every player wants confidence that each layer is acting responsibly when it comes to security and data privacy.

Using a cloud-based platform enables the sharing of information within the ecosystem. As the capabilities advance, the ability to share and re-use assessment elements can reduce the need to answer detailed questionnaires provided by each customer.

We believe by instilling confidence in our existing and potential customers from a security standpoint, we have a competitive advantage.

UNIVERSITY OF WISCONSIN - MADISON

BOB TURNER

Chief Information Security Officer

COMPANY OVERVIEW

The University of Wisconsin-Madison is a public research university in Madison, Wisconsin. Founded when Wisconsin achieved statehood in 1848, UW-Madison is the official state university of Wisconsin, and the flagship campus of the University of Wisconsin System. It was the first public university established in Wisconsin and remains the oldest and largest public university in the state.

UW-Madison is organized into 20 schools and colleges, with approximately 30,000 undergraduate and 14,000 graduate students. The University employs over 21,600 faculty and staff. Its comprehensive academic program offers 136 undergraduate majors, along with 148 master's degree programs and 120 doctoral programs.

UW-Madison is also categorized as a Doctoral University with the Highest Research Activity in the Carnegie Classification of Institutions of Higher Education. In 2017, the university ranked 6th in the nation in terms of research expenditures.

BUSINESS USE CASES

Many universities, including University of Wisconsin-Madison, conduct a considerable amount of research containing proprietary or sensitive information. It is the university's responsibility to ensure this information is protected. Organizations paying for the research expect it to be kept safe, thus requiring us to demonstrate how our internal controls will protect their data. In the parlance of third-party risk management, the University of Wisconsin-Madison is primarily the third party in a research environment.

When under contract with a federal or corporate entity, we are asked to provide a certification dictating our controls meet their standards. The government asks for compliance with the federal acquisition regulations, and that private companies provide their own questionnaires for us to answer. For continuity purposes we use the NIST cybersecurity framework as a guideline. We use 124 items in the framework and compare it with the actions we perform in order to provide a report on how we handle sensitive data.

What makes TPRM difficult at the university level is the ecosystem consists of nearly two dozen different business entities. Each of the colleges have aspects of their research that makes security and third-party relationships unique. It is up to the TPRM process to address these differences while presenting a unified university position.

In addition to providing our security posture, we are also required to conduct third party assessments on our suppliers. Those suppliers are primarily cloud-based technology vendors we use to process sensitive data. It is the security office's responsibility to conduct cybersecurity focused risk assessments that zero in on data protection activities. For these assessments, we rely on the Higher Education Community Vendor Assessment Toolkit (HECVAT), which provides standard questions dealing with issues such as data encryption and access management associated with hosted data.

Bottom line, we are involved in third party risk management from both sides of the process.

BUSINESS GOAL IMPLEMENTING THIRD PARTY RISK MANAGEMENT

The guiding principle behind our TPRM operations is to protect the university's reputation and be the best steward for the university's resources. Our fundamental goal is to avoid putting our data at risk to exposure. We are responsible for protecting data held by our partners which could result in damages for contract violations if we do not understand and mitigate against the potential risk exposure.

Protecting the data entrusted to us by our research partners is good business. There are business incentives that accrue when we safeguard research sponsor's data as it leads to more business. When governments and private companies have confidence in our security operations, they are likely to continue funding research.

The university is a member of the Big Ten Academic Alliance. In 2018, the CISOs of the member institutions pooled resources to provide vendor risk management services and develop a shared platform. The platform assists member universities in evaluating the security risk of third-party software and provides a mechanism to share security assessment information. A member of the University of Wisconsin–Madison can share risk assessments we conduct and have access to evaluations conducted by the other institutions. Through this collaborative effort, we can benefit from their analysis.

KEY FACTORS TO CONSIDER

The first element in TPRM we look for is adaptivity. Primarily, this refers to the ability of the tool to adjust to our security framework. We have adopted a derivative of the NIST Cyber Security Framework, and the HECVAT questionnaire framework is given to cloud solution providers to confirm that information, data, and cybersecurity policies are in place for protection.

The second factor is efficiency. Assessments must be done quickly, as oftentimes there is a short window to complete the paperwork required with the security plan supporting a grant or research project. When the university needs an investigation completed, the security staff must collect information, analyze it, and provide a completed risk assessment. Using a TPRM tool, the HECVAT, and leveraging prior assessments conducted by other Big Ten universities can vastly improve overall process efficiency.

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

On the technology front, comprehensive data management is most important. Managing the sharing of data for TPRM is a daunting task. A file sharing capability that allows our third parties to deposit their data into specific folders and compartmentalize the data locations is critical to data protection. Files must also be free of viruses. Lastly, we require the system to alert us when documents are uploaded.

We use a cloud-based SaaS product because of its easy accessibility, but within the platform we insist on strong authentication, encryption, and auditing. We need to know exactly who has accessed data. User accounts need to be self-serviced, allowing the creation and close of user accounts without a convoluted permission process administered by a help desk.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

The greatest asset from our TPRM solution is valuable reporting. The vendor assessment reports provide the profile with a ranking of high, moderate, and low risk. It is used in purchasing decisions and can help manage the relationship over time, allowing leadership to make informed decisions. We also use existing reports as a template when evaluating similar products and when we are the third party.

IMPACT ON STAFFING LEVELS

We hired additional staff to handle our third-party risk process, however this increase in staff may not be permanent. There must be a business justification for the expense and a demonstration that the risk management activity has a quantifiable return. As any process, we expect to evaluate this investment frequently.

PEER RECOMMENDATIONS AND ADVICE

If you are not conducting third-party risk assessments of your suppliers, especially managed service providers, you are placing your organization at risk. You need to understand the risk to your organization when you share critical information with others. Understanding how well a company protects your data should be part of the contract decision process. As a security leader, you are obliged to provide business leaders information on the potential of data loss or exposure associated with a given supplier.

Handling third party assessments is not a difficult process, provided you have the right tools and the correct approach. You must scrutinize the answers you receive as part of the questionnaires, and challenge the information to gain additional insight.

Finally, like any other risk management effort, you must be willing to invest time and resources into the process in order to gain value from the activity.

SUMMARY

Organizations should have a Third-Party Risk Management program to ensure adherence to your contractual obligations and protect data. Ranking suppliers with high, moderate, and low risk provides important insight regarding purchasing decisions and can help manage relationships over time.

Protecting data is good business. You must be serious about the program. Using a cloud-based SaaS service provides an infrastructure that can benefit your efforts. Customers are much more likely to return when they have confidence that your security operations are designed to minimize the risk of exposure or a data breach.

WOODFOREST NATIONAL BANK

MARC CRUDGINGTON
SVP Information Security & CISO

COMPANY OVERVIEW

Woodforest National Bank is one of the strongest community banks in the nation, proudly offering quality customer service since 1980. Woodforest offers both consumer and small business products and services. Woodforest Commercial Banking team offers products and services in the areas of Credit and Financial Services, Wealth Management, Cash Management, Merchant Services, and more. Mobile banking is also available.

Privately owned Woodforest National Bank is headquartered in The Woodlands, Texas with 750 branches located in 17 states across the United States. Woodforest has over $7.0 billion in total assets.

BUSINESS USE CASES

Woodforest National Bank is in a highly regulated industry so the overarching business use cases for the bank's Third-Party Risk Management (TPRM) program are to support audit, security and mandated compliance requirements. Vendor risk scoring tools provide valuable information on third parties with whom regulated data is shared.

The third-party assessments are part of a larger life-cycle management program and key component of our cybersecurity efforts. For the bank, safeguarding our customers and their data is paramount. As third-party breaches could directly impact the bank, it is business critical to ensure that the security of the third party, be it a partner, vendor or supplier, does not only meet compliance requirements but the bank's security standards.

In addition to the third party's security posture and potential risk exposure to the bank to, it is imperative that we have visibility into the viability and health of our partners, vendors and suppliers. A number of our customer services are supported by applications created or operated by other parties. If the partner, vendor or supplier is not financially stable and/or has reputational issues and fails that could directly impact the bank's ability to perform specific business.

BUSINESS GOALS IMPLEMENTING THIRD PARTY RISK MANAGEMENT

The overriding business goal is to understand the inherent risks when engaging with another companies. The risks from can range from financial to operational to reputational to regulatory to cybersecurity. As CISO, I am tasked specifically with assessing the ability of the bank's technology vendors to secure data. This covers both customer and employee information.

The cybersecurity component of Woodforest National Bank's TPRM activity feeds into our consolidated vendor management life cycle solution. Conducting assessments in a timely manner allows us to determine whether to onboard a vendor. It also enables us to conduct on demand risk assessments to provide a snapshot of the third party's cybersecurity posture.

KEY FACTORS TO CONSIDER

TPRM is a necessary component of an effective security program. At Woodforest National Bank we have been performing them for a considerable amount of time. Having a well-established methodology to gauge the potential risk to the bank allowed us, when we opted to leverage a security assessment tool to incorporate automation, we were in good stead in terms of knowing the criteria such a system needed to address. Top amongst those is the system had to be highly customizable so it could handle the bank's robust workflow process. We were unwilling to significantly modify the process created over a number of years to accommodate the tool, the tool had to accommodate the process. Additionally, the third-party assessment tool had to be able to easily import our existing vendor information.

Out-of-the-box functionality also was important. The more features that could be adopted directly without customization increases the value of the tool. Additionally, it was important that the monitoring of the vendor was continuous, and we received automated notifications with changes to their risk rankings.

Finally, for Woodforest National Bank, when selecting a TPRM solution it was important that the vendor committed to innovation and product improvements as well as a consistent product development life cycle. Most TPRM products are cloud-based so it is preferable to engage a company that releases updates with consistent frequency. Also, selecting a vendor that is aware of your industry's particular requirements, for the bank that was regulatory mandates, will be beneficial in getting the most value out of the product.

KEY TECHNOLOGY COMPONENTS WHEN FIELDING TPRM

Using a cloud platform is the based TPRM solution is optimal as the bank did not have to maintain the software and hardware required to operate it. As the TPRM solution provider space is becoming more established, those systems are already in place.

For Woodforest National Bank cloud is the best delivery method however the products should have open application programming interfaces (API) which allow customized and other risk management components to be incorporated into the overall system.

OUTCOME AFTER IMPLEMENTING A TPRM SOLUTION

As a financial institution Woodforest National Bank must annually evaluate the risks to our operations associated with tier one and tier two vendors. For us this consists of about 200 or more tier one and tier two third-party vendors. Given there are over 250 workdays in a year it is considerable work to keep these evaluations up to date. Adding a customizable TPRM solution with automation built in has significantly increased the efficiency of the process.

While having an effective procedure is important, the primary outcome of our TPRM activities are to provide our executive team across the organization important information on risks to the bank that are attributable to our partners, vendor, and suppliers. Our TPRM solution provides continuous and in-depth visibility into our vendors, partners, and suppliers. The solution creates executive summaries that rank the overall risk of each vendor, partner, or supplier. With this information, for example a score between 1 to 100, executives are given the information they require to understand the potential risks to the bank.

A key outcome of the TPRM solution has been improved process efficiency, better reporting, and timely information to the executives and/or vendor owners who need to make decisions about the risks attributed to third party vendors.

IMPACT ON STAFFING LEVELS

Implementing a TPRM solution did not increase staffing but rather added a tool that improved the overall process. In addition, this has increased our staff's productivity as the TPRM solution has freed up members of our team to focus on their primary role by reducing the amount of time required to chase paperwork.

PEER RECOMMENDATION AND ADVICE

Third party risk management is a must have for the business. It is not limited to the security function but cuts across all business lines. Depending on the business unit impacted from audit to legal to HR, the decision makers and employees interacting with the partner, vendor or supplier need to be involved in the decision to on board and the regular assessments to identify any changes to the risk profile. Whether you augment your TPRM solution with a third party offering or not, in order to be valuable, the TPRM program needs to be part of the business process.

Manually assessing Woodforest National Bank's over 200 vendors that need to be reviewed annually and managing the other Tier 3 vendors was no longer feasible. Using a product that provides efficiencies and visibility into how particular vendors impact your risks not only improved our productivity it was highly cost effective.

SUMMARY

Third party risk management is a must have activity for your business. It is required to ascertain which vendors you should be sharing data with, especially if you are in a regulated sector such as the financial industry. At Woodforest National Bank we take a holistic approach to risk by our partners, vendors, and suppliers. We look at the potential financial, operational, reputational, regulatory, and cybersecurity components as we assess the inherent risks associated with our third parties the potential risks to which they would expose us.

We opted for a cloud based TPRM solution that provides automated efficiencies, enhanced workflows, and valuable reporting. Having an effective procedure is important as well as being able to take that information and share it with the key stakeholders and the bank's executives so they can make informed decisions on who to do business with.

PLATINUM SPONSOR

BLACK KITE

Black Kite reduces the uncertainty of your cyber risk with a high quality platform that does the work for you. Created from a hacker's perspective, we're not another cyber rating tool. Our platform tells you which vendors pose the highest risk to your company without creating more labor on your end. The platform is scalable, all-encompassing, and tailored to identify your problem areas. Black Kite is also the ONLY cyber risk rating system that can measure the cost associated with a potential third party cyber breach. Know the risk every organization in your ecosystem poses in dollars and cents. Learn more at www.blackkitetech.com

LEAD WRITER

MIKE DAVIS

CISO, alliantgroup

As Chief Information Security Officer (CISO), Mike operationalizes Data Security, Privacy, & Risk Management while advising leadership on protecting critical information resources and managing an enterprise cyber security portfolio. As CISO, his mission includes executing a risk-based security strategy that supports enabling the company's success objectives by securing and protecting both sensitive company and client information.

An experienced cyber security professional with 20+ years in diverse leadership positions: CISO, Senior Cyber Technical Authority, Cyber Security / Risk management consultant, Cyber Program Manager, and Chief Systems Engineer, among others. Mike is also a retired U.S. Navy Engineering Duty Officer and Federal Government employee (GS-15).

Mike supports several security associations: the FBI InfraGard, SD IEEE (Cyber SIG), ISSA/ISC2, and ISACA among others. His certifications are: CISSP, CISO, and Systems Engineering, along with senior qualifications in Program Management and Risk Management, and holds a MS in Electrical Engineering and a MA in Management.

EXECUTIVE EDITOR

BOB TURNER

CISO, University of Wisconsin-Madison

Bob Turner is the Chief Information Security Officer at the University of Wisconsin-Madison where he leads the development and delivery of a comprehensive information security and privacy program.

His previous experience includes managing consultants focused on cybersecurity policy and compliance with assessment of information systems and cyber security inspection as principal strengths.

Bob also served in the U.S. Navy as a Communications Officer with a 23-year career in telecommunications and information systems management.

He earned BS and MS degrees in Management and Information Security and is a Certified Information Systems Security Professional and with National Information Assurance Training Standard certificates as a Senior Systems Manager and Systems Certifier issued from the Naval Post Graduate School.

EDITOR

MARC CRUDGINGTON

CISO, SVP Information Security for Woodforest National Bank

Marc Crudgington is the Chief Information Security Officer, SVP Information Security for Woodforest National Bank and in the role since joining Woodforest in August 2012. Marc is a veteran of the United States Air Force serving honorably from April 1992 – April 1996; he held a Top-Secret clearance and performed duties in intelligence, computer operations, computer communications, and network communications. Prior to Woodforest, Marc worked for Advantage Sales and Marketing, KPMG, and Silicon Valley technology companies with leadership roles in IT and engineering. Marc has a Master of Business Administration, Technology and Strategy, from the University of California Irvine – Paul Merage School of Business and a Bachelor of Business Management from the University of Phoenix. Marc also attended the FBI CISO Academy in March 2017. He holds a Secret Clearance and PCIP, ISA, CRISC, Security+, Scrum Master, and ITIL certifications; previously he held a C|CISO, PMP, TOGAF, CISM and CISA certifications.

Marc serves on the University of Houston CIS Industry Advisory Board, Sam Houston State University Digital and Cyber Forensic Engineering Advisory Board, Lone Start College Cybersecurity and Compute Science Advisory Board, Optiv Customer Advisory Board, InfraGard Houston Chapter Board of Directors, Texas Banker's Association Technology Committee, Community Bankers Association Privacy/Data Security Working Group, and several cyber-security and technology conference advisory boards. Previously Marc was part of the National Infrastructure Protection Plan Working Group and DHS Threat Information Sharing Framework Working Group. Marc is a member of InfraGard and previously served as the Deputy Chief for the Houston Chapter Financial Services CSC. Marc has been a contributor and posted several articles, presentations and white papers on LinkedIn, for the Project Management Institute, and a speaker, panelist, and moderator at several IT and Security conferences. In 2019 Marc was nominated, selected as a finalist, and won the coveted T.E.N. ISE North America Executive of the Year – Financial Services award. In 2019, Marc was nominated and selected as a finalist for the T.E.N. ISE (Information Security Executive) Central Executive of the Year award and was nominated for the ISE Central People's Choice award. In 2018 Marc was nominated for and a finalist for the T.E.N. ISE North America Executive of the Year award and the T.E.N. ISE People's Choice award; in 2016 Marc was nominated for and a finalist for the T.E.N. ISE Central Executive of the Year award and T.E.N. ISE Financial Services Executive of the Year award.

EDITOR

AL GHOUS

CSO and Head of Security, ServiceMax

Al Ghous is the CSO and Head of Security at ServiceMax, a Cloud platform focused on field service management and automation. Prior to ServiceMax, Al was responsible for Platform, Product and IoT security at GE Digital. Al has been in the Cyber Security industry for over 18 years contributing in different capacities from Product Security and Risk Management to Solution Consulting and Security Architecture. He has held other leadership roles in organizations such as Ernst and Young, Oracle, Kaiser Permanente, and Informatica to name a few.

Al is active in the Cyber Security industry and part of several industry organizations and consortiums, as well as a member of several advisory boards. As an Advisor, Al takes pride in helping Founders focus on product development while maturing their Security posture to attract customers and investors alike.

EDITOR

NIKK GILBERT

CISO, Cherokee Nation Businesses

Nikk Gilbert is the Chief Information Security Officer for Cherokee Nation Businesses. Cherokee Nation Businesses is the economic engine of Cherokeee Nation, the largest Indian Nation in the United States. Cherokee Nation and its businesses employ 11,000 people. CNB owns companies in the gaming, hospitality, information technology, health care, personnel services, distribution, manufacturing, telecommunications, environmental services and security and defense industries.

With 20 years of executive-level experience in Information technology roles, Nikk is a respected thought leader within the government & private sectors. Experienced in multiple verticals, (financial services, manufacturing, oil & energy, government & military), He is focused on building success by understanding the needs of the customer, and by enabling the business through a deep understanding of the corporate strategy and its culture.

Nikk's experience includes working as an information security executive (CISO, CSO) & information technology leader (CIO) for large multinational organizations such as the American Department of Defense, NATO, Alstom, ConocoPhillips and the U.S. Navy.

Nikk is a recipient of the US Navy's Meritorious Civilian Service Medal, holds the CISSP and CISM security certifications and has been a keynote speaker at technology events throughout the world.

EDITOR

JOEY JOHNSON

CISO, Premise Health

Since 2009 Joey Johnson has served as the Chief Information Security Officer at Premise Health, the nation's leading provider of direct access employer sponsored health and wellness centers for employees with nearly 650 facilities across America. In 2016 Joey was recognized as the Nashville CISO of the by the Nashville Technology Council, followed by being recognized the 2017 Southeast US Security Executive of the Year, and finalist for the 2017 North America Security Executive of the Year. He served as a 2018 judge for the Technology Executives Network Southeast security executive of the year, and also at the National level as a judge for the 2018 North America Security Executive of the year for each of the healthcare, financial, retail/manufacturing, and education sectors. The Premise Health security operations team was recognized by CSO Magazine as winner of the 2018 CSO50 awards for having one of the top fifty national cybersecurity projects for the year.

At Premise Health Joey is responsible for leading all organizational efforts related to security operations and engineering, security monitoring and incident response, information technology and security compliance, identity access management, policy development, security audit, third party risk management, and physical security to meet challenging security and compliance demands. In his eight years with Premise Health, Joey has been instrumental in implementing a proactive security and risk management environment focused business alignment, organizational risk awareness, and positioning security as a business enabler that is transformative in the healthcare industry.

Prior to joining Premise Health, Joey was the Chief Security Officer for the United States Department of Commerce, Office of Computer Services. He has over 20 years of experience in the cyber-security industry including leadership roles in both the public and private sectors, with a focus on organizations in the federal government, defense, information technology, healthcare, and transportation industries.

Black Kite

Company Overview

Our mission is to deliver automated cyber risk results so you can make better business decisions. Black Kite's high quality data platform does the work for you. Created from a hacker's perspective, our platform provides an all-in-one assessment by combining cyber security ratings, compliance controls, and potential financial loss calculations for every vendor in your ecosystem. Black Kite is also the only cyber risk rating system that enables enterprises to measure the probable financial loss from a cyber attack.

Contact Information

John Sullivan
Sr. Vice President of Sales
978-870-6640
john.sullivan@blackkitetech.com

Paul Paget
CEO
781-771-1929
paul.paget@blackkitetech.com

Solution Description

Black Kite is not another cyber rating tool. Our platform tells you which vendors pose the highest risk to your company without creating more work. Boards and CEO's are liable. We try to make it as easy as possible to communicate problems to the people who need to know about them. Black Kite's platform identifies risk areas that REQUIRE attention, and provides easy-to-understand feedback to address them. Get answers around the uncertainty of your cyber risk more quickly, cost-effectively, and on a continuous-basis.

Mandatory Requirements

Requirement #	Feature		Description
M-1	Non Intrusive Scan	From a hacker's perspective, a scan of web & dark web company presences with detailed findings based on cyber threat intelligence.	Yes. Black Kite uses open-source intelligence and non-intrusive scans to assess your cyber risk without ever touching the target customer. It collects information across 19 cyber categories and a digital footprint.
M-2	Financial Impact	Leverage a standard like the FAIR (fairinstitute.org) cyber risk quantification model to calculate the probable financial impact ($$) of a cyber event caused by a third party. Capability must be able to be applied to all vendors.	Yes. Black Kite leverages Open-FAIR to calculate the probable financial impact of a cyber event caused by a third party. The functionality is scalable and can be applied to all vendors easily
M-3	Centralized Dashboard	Single Dashboard containing all the information from Technical, Compliance, Financial perspectives. The Dashboard must allow C-Level users to have a full view of company's cyber risk posture on a single page and to Technical users the ability to dive into the findings and implement remediation suggestions. Outputs can be extracted to a Spreasheet or a document for distribution.	Yes. Black Kite's Company overview dashboard provides a 3D view of technical, compliance and financial impact in a single view. All findings can be examined in detail and all come with remediation suggestions. Outputs can be extracted to a spreadsheet or document
M-4	Sharing Editable results with a Vendor	All findings should be able to be shared with a vendor and vendor should have access to the findings and have the abiliity to review all findings and take corrective actions. Vendor should not have to be a customer of cyber rating service vendor in order to receive and remediate findings	Yes. All findings can be shared with a vendor at no charge. The vendor can review the findings and take corrective actions. Furthermore, Black Kite will assist the vendor if needed. Vendor does not need to be a Black Kite customer to receive assistance.
M-5	Near Real-Time Alerts	New findings should appear in the platform's dashboard as soon as it is publicly discoverable (via OSINT sources).	Yes. All data in Black Kite is collected as soon as it is available. As it aggregates and collects information from various OSIT sources, the information is presented via dashboards and presents findings in a realtime fashion.
M-6	Prioritisation of Assets and Findings	Assets identified as critical vulnerablities and related findings must be able to be prioritised for immediate actions.	Yes. Black Kite prioritizes critical findings automatically. The dashboard shows the top 10 riskiest findings and has hot links embedded in the view to provide detailed analysis on the critical issues that need to be flagged for immediate response. Further, Black Kite's strategy reports detail how much ratings will improve based on specific remediation actions taken.
M-7	Discovery Footprinting	Digital footprint should include all registered domains, sub domain sand assigned/used IP addresses with daily updates. User should be able to exclude exceptional assets like honeypots, malware sandboxes, guest networks and BYOD networks. User should be able to remove implausible items from (and add new assets to monitor to) the scorecard.	Yes. Black Kite compiles an organization's digital presence on the web. This process is part of the initial and continuous asset discovery delivered in the digital footprint category. The digital Footprint includes domains (Active or Dormant), Subdomains, IP addresses, CIDR blocks, services, etc.. Like any other module in the Black Kite platform, it is customizable to the customer's requirements. Whether you need to manually add a domain/IP or exclude an asset that is part of a Sandbox or honey pot, all can be done with the click of a button.
M-8	API Integration	Scans should be able to be initiated via API and the platform interface. The content returned by API should be able to include the high level data but also the details of each finding. API should allow integration with other solutions (i.e. Splunk, QRadar, etc.).	Yes. Black Kite provides an at-rest API as part of its platform. There is no additional charge to utilize the APIs.
M-9	Role-based Access	Access to portal and features should be limited or expanded based on the type of role or function a user has within the system	Yes. Black Kite has built-in Role Based Access Control. The RBAC can vary depending on the roles: • Sub-Root: Full control (Read/Write) over multiple instances • Super Admin: Full control (Read/Write) within an instance • Super User: Read-only within an instance Ecosystem Admin: Full control (Read/Write) within an Ecosystem or Ecosystem User: Read-only within an Ecosystem These roles can be adjusted to ensure all members within the organization have the appropriate access within Black Kite platform.

Additional Requirements

Requirement #	Feature	Description	Yes/No/Partial	Vendor's Comments
AR-1	Knowledge Base	Based on standards like NIST, MITRE (CTSA, CWRAF, CVE, CVSS, CWSS) etc. with the description and impact of the problem and remediation recommendations.	Yes	All Knowledge base articles map to industry-accepted standards (NIST,MITRE,FIPS,FISMA,etc...)
AR-2	Compliance Check	Measure the compliance level of a company based on widely used and recognized frameworks. Pre-populated compliance report for NIST, ISO27001, GDPR with possibility to collaborate and upload & share compliance reports.	Yes	All compliance frameworks are supported (NIST, ISO 27001, GDPR ,etc..). Black Kite also has the ability to add custom questionnaires upon request.
AR-3	Financial Impact	Ability to calculate the probable financial impact if a cyber event were to occur at the Company or at a third party in order to cost-effectively achieve and maintain an acceptable level of loss exposure.	Yes	Black Kite provides customers with a Probable Financial impact (Based on the FAIR model) to put risk into dollars in the event a vendor suffers a cyber event or breach. Simulations in the platform can be done to understand different risk scenarios and to best represent the customer's relationship with a vendor.
AR-4	Technical Risk	Ability to identify technical risk in commonly assessed categories, such as Email Security, Application Security, Network Security, and Website Security.	Yes	Black Kite points out vulnerabilities and attack patterns using 20 categories and more than 400 controls, without ever touching the target customer.
AR-5	Risk Scoring	Uses common frameworks to score risk (e.g., CVSS, ISO, NIST CSF) and includes measurements of * Asset Criticality (discover and classify) * Threats (events perpetrated by threat actors in the context of the critical assets and vulnerabilities) * Vulnerabilities (weaknesses in the infrastructure) * Controls (mitigating controls against the vulnerabilities) * Likelihood of a Breach (historical projected) * Impact of a Breach (business assessment based on CIA triad)	Yes	Black Kite is based on Frameworks and standards (CWSS, ISO, NIST, etc..). It leverages OSINT data to aggregate and score a 3rd party delivering an unbiased, standards based review of vendors to better assess risk. All measurements listed in the requirements are out of the box functionality.
AR-6	Multiple scan-type option	Ability to scan a vendor in order to quickly gain insight into their risk posture. Additionally, the ability to initiate a deeper scan in order to get a comprehensive look at a company's security and risk posture.	Yes	Black Kite leverages its data to provide a 90 second rapid assessment of any vendor based on the input of their main domain. It can also provide a full comprehensive report in an average of 90 minutes.
AR-7	User Accounts	Unlimited User Access available	Yes	Black Kite does not limit the number of accounts that can be tied to a certain customer ecosystem.
AR-8	Identity and Access Management	Supports common IAM strategies	Yes	Supports detailed role-based access controls and encryption
AR-9	Robust Reporting	Ability to export all facets of the results, including technical and complaice reports. The ability to summarize reports or provide a full, in-depth reports should be available. Reporting should be both interactive and static.	Yes	Reporting out of the box is robust and expansive. Black Kite offers reports for the internal stakeholder, vendor, executives, etc.. They can be exported with a click of a button or be set up to be delivered on a schedule.
AR-10	Company Benchmarking	Ability to compare one company to one or more companies/ peers over time	Yes	Detailed benchmarking is included
AR-11	Industry Benchmarking	Ability to compare a company's score or risk to their industry over a period of time.	Yes	Detailed benchmarking is included
AR-12	Snapshots/Trend	Ability to easily review a company's risk posture over time with the ability to drill down into past reports for comparison	Yes	Can review risk posture over time and drill down into past reports

Pricing Model

Feature	Description	Metric	Annual Price
Company Self Monitoring	Continuous Comprehensive (Annual Subscription)	1 Entity	$ 2,995.00
Continuous Third Party Monitoring	Pricing based on the number of Vendors to be Continuously monitored (Annual Subscription)	Entity	6 Entities $5,970.00 11 Entities $9,851.00 100 Entities $54,725.00 1,500 Entities $223,875.00
Peer Reviews (benchmarking)	Pricing based on the number of Vendors to be Continuously monitored (Annual Subscription)	Entity	6 Entities $5,970.00 11 Entities $9,851.00 100 Entities $54,725.00 1,500 Entities $223,875.00
Merger & Acquisition targets	Pricing based on the number of Vendors to be Continuously monitored (60- Day Subscription)	Entity	10 Entities $2,995.00 100 entities $15,600.00

Black Kite

Business Requirements

ID #	Requirement(s)	Vendor Response	Vendor Comments	
B-1	Is the solution cloud-based or installed on-premise?	Cloud based		General Business Requirements
B-2	Does the system provide the ability to configure workflow for onboarding without customization or assistance from vendor?	Yes		
B-3	Does the solution calculate inherent risk based on rules?	Yes		
B-4	Does the system allow for the uploading of documents provided by employees and external vendors?	Yes		
B-5	Can the solution track all correspondence between the vendor anywhere in the vendor lifecycle process/workflow?	No		
B-6	Describe how the system tracks fourth-party relationships.		Black Kite automatically discovers the IT vendors of an entity (4th parties). It is also possible to add auto-discovered 4th parties to a desired ecosystem with a click of a button.	
B-7	Please describe how historical assessments are stored and accessed.		Black Kite licenses its platform via a continuous monitoring model. Once a cyber ratings scan is initiated, Black Kite collects, reports and alerts on the entity continuously. Historical data is kept on all entities being monitored	
B-8	Does the solution provide capabilities to request more information from the vendor that may be outside the original due diligence questionnaire?	Yes		
B-9	Does the system provide capabilities to track Service-Level Agreements (SLAs)?	Partially		
B-10	Does the software send SLA metrics to vendors to document responses and attach evidence? Please describe this process.	No		
B-11	Does the solution support performance reviews sent to relationship managers?	No		
B-12	Is there an online/cloud portal for Vendors?	Yes		Vendor Portal
B-13	Do vendors maintain their own passwords for the portal?	Yes		
B-14	Can vendors export their questionnaire to complete offline as needed? Can completed responses be imported back into solution in an automated fashion? Please describe.	Yes	Questionnaires are easily exported and imported as excel spreadsheets	
B-15	Can vendors delegate or invite additional associates into the solution to assist with assessments?	Yes		
B-16	Is there a way for vendors to access a report of all open issues?	Yes		
B-17	Do vendors receive alerts of upcoming due dates, past due assignments and other actions?	No		
B-18	Can vendors provide status updates to issue resolutions?	No		
B-19	Do you allow vendors to import a completed SIG without requiring copy/paste on a question-by-question basis (one-click import)?	Yes		
B-20	Does the vendor have the ability to complete the questionnaire and upload/attach documents?	Yes		
B-21	How does the vendor see summary of questions and anything that is incomplete?	Not Possible		
B-22	Can vendors save their work and complete it at a later time/date?	Yes		
B-23	Can workflow be created/modified without customization or assistance from your professional services organization?	Yes		Workflow
B-24	Can the status of all workflow steps be tracked and reported on?	No		
B-25	Describe how workflow steps can be advanced or rejected.	Yes	We provide enough data points for the stakeholder and vendors to advance their work flow to operationalize there vendor assessment process into a more though and automated process	
B-26	Can workflows be modified at any point in time without requiring professional services?	Yes		
B-27	Will the system allow multiple departments with different access permissions to access the solution?	Yes		Administration
B-28	Please describe how role-based access profiles are configured within the system.	Yes	RBAC can be configured when setting up a user account. This role assignment can also be changed at any time.	
B-29	Can the solution assign alerts/notifications/tasks (systematically) to employees or vendors?	Yes		
B-30	Can our organization create questionnaires whenever needed without assistance from vendor/professional services?	Yes		

ID #	Requirement(s)	Vendor Response	Vendor Comments	
B-31	Can our organization incorporate/append/modify SIG content in our questionnaires?	Yes		Administration
B-32	Does the solution provide the ability to add/create/modify risk assessment (questionnaires/ templates) to include a scoring methodology?	No		
B-33	The scoring methodology must include three options: Inherent risk score = after risk assessment has been completed and before controls are in place. Critical Vendor = score based on responses from the risk assessment. Residual risk score = after risk assessment AND due diligence assessments have been completed (after controls are in place). Please describe how you support this.	Black Kite's scoring methodology provides an inherent risk score on any company in 60 seconds. Black Kite identifies critical vendors by ranking via technical data, compliance posture and financial impact. Black Kite delivers a residual risk score by giving each vendor a playbook (Strategy reports) to follow for remediation and score improvements.		
B-34	Does the solution provide the ability to assess the risk, by including scoring, of the vendor relationship based on the questionnaire responses?	Yes		
B-35	Can the system map questions back to standards, controls, risks and other business records?	Yes		
B-36	Does the system provide capabilities for multiple approvals based on the assessed risk score after due diligence assessments are completed by subject-matter experts (SMEs)?	No		
B-37	Does the system auto-scope questions to include for a vendor based on service or other data criteria?	No	Questions for vendors are based on Frameworks on Shared assessments (SIG).	
B-38	Does the solution securely send questionnaire(s) to the vendor via the system?	Yes		
B-39	Can notifications be managed/modified without professional services help (via system configuration)?	Yes		
B-40	Please describe how the system supports escalation emails.	Emails are sent at the time of scan completion, when a report is delivered or an alert has been triggered. These delivery methods are all customizable		
B-41	Does the system provide the ability to add a property/field at any point in time without requiring professional services?	No		
B-42	Can the solution be branded to include logos and company color scheme?	Yes		
B-43	Can we import data through the solution without professional services?	Yes		
B-44	Can we mass update data through solution without professional services?	Yes		
B-45	Please describe your system's ability to integrate with other systems. Please describe the level of integration possible or if there is and API available.	A restful API is provided making integrations straight forward		
B-46	Is scoring in the solution configurable? (It does not require any custom code.)	No		
B-46	Does the system provide canned/out-of-the-box reporting?	Yes		Reporting
B-46	Does the system provide user-configurable reporting?	No		
B-46	Does the system provide a dashboard view, at profile level, of activities and reporting?	Yes		
B-46	Can we produce reports in various formats such as Excel, Word, and CSV?	Yes		
B-46	Does the solution integrate with business analytics tools (such as Tableau)?	No		
B-46	Can we define our security rules?	No		Security
B-46	Is security role-based?	Yes		

Technical Requirements

ID #	Requirement(s)	Vendor Response	Vendor Comments
T-1	Does the system support single sign-on for all functions performed by users? (Additional logins are not required when switching between various application modules.)	Not currently. On 2020 roadmap	
T-2	Does the solution support external role management via identity access management (IAM) automation tools?	No	
T-3	Does your organization publish SLAs covering availability, transaction time, storage, performance, and support requests received from the customer? (Please include Service Level Metrics with your response.)	Not publicly available but Black Kite can share the uptime robot statistics as required.	
T-4	Do you have published minimum system requirements for any client and server software components that must be installed as part of the solution. Specs must include CPU, memory, storage throughput, and storage space. Please include these specs with your response.	Not Applicable. Black Kite is a Cloud based solution	
T-5	Does the solution support Internet Explorer 11 or higher for web-based components?	Yes	
T-6	Does the solution leverage native browser functionality? (It requires no additional plugins (Flash, Silverlight, etc.)).	Yes	
T-7	Do we have unlimited access to data generated by the application. Data is accessible via data exports, direct database access, or some other automated means.	Yes	
T-8	Does your organization have established windows during which any maintenance is performed?	Yes	
T-9	Does the solution include a replicated lower-level environment for development and testing activities?	No	
T-10	Please provide an application roadmap that includes all major system enhancements over the next 3 years.	Detailed roadmap will be provided after a Mutual NDA is put in place	
T-11	Does your organization publish a reference architecture that defines an ideal installation for all system components? Includes both on-premises and cloud solutions.	Only Cloud based and we do publish high level architecture. Detailed architecture provided with Mutual NDA in place	
T-12	Does your organization have a formalized mechanism for sending system data using SFTP? Note: Any secured protocol. Encryption is preferred.	Yes, if we need to send data we only use strongly encrypted channels. TLS1.1 or above and only SSH or SFTP or HTTPS	
T-13	Can your organization deliver data which resides in system with a file format that is delimited by or some other customer delimiter?	Yes, findings are exportable in CSV (comma delimited). Custom delimiter is not available.	
T-14	Are data elements well documented? Is there a data dictionary available for ease of use and integration?	Yes, Black Kite publishes its knowledge base on its Zendesk help page. API and postman interface of all APIs are also available in the help pages.	
T-15	For employees, does the system support multi-factor authentication?	Yes	
T-16	For vendors, does the system support multi-factor authentication?	Yes	
T-17	Do you allow/support/enforce IP restriction, so that we can ensure that only users in our network are accessing the system (excluding the members application process)?	Yes	

General Technical Requirements

RFI Template for CISOs Investigate: Third-Party Risk Management (TPRM)

Company Name

Company Overview *(1 Paragraph -- 100 words)*

Contact Information *Name, Title, Phone, Email*

Solution Description *Solution Description (Narrative not to exceed 1/2 page -- 250 words)*

Mandatory Requirements

(Must Have)

Requirement #	Feature		Description
M-1	Non Intrusive Scan	Non-intrusive scan of web & dark web company presence with detailed findings based on cyber threat intelligence like an hacker	Yes
M-2	Financial Impact	Leverage a standard like the FAIR (fairinstitute.org) cyber risk quantification model to calculate the probable financial impact ($$) of a cyber event caused by a third party. Capability must be able to be applied to all vendors.	Yes
M-3	Centralized Dashboard	Single Dashboard containing all the information from Technical, Compliance, Financial perspectives. The Dashboard must allow C-Level users to have a full view of company's cyber risk posture on a single page and to Technical users the ability to dive into the findings and implement remediation suggestions. Outputs can be extracted to a Spreasheet or a document for distribution.	Yes
M-4	Sharing Editable results with a Vendor	All findings should be able to be shared with a vendor and vendor should have access to the findings and have the abiliity to review all findings and take corrective actions. Vendor should not have to be a customer of cyber rating service vendor in order to receive and remediate findings	Yes
M-5	Near Real-Time Alerts	New findings should appear in the platform's dashboard as soon as it is publicly discoverable (via OSINT sources).	Yes
M-6	Prioritisation of Assets and Findings	Assets identified as critical vulnerablities and related findings must be able to be prioritised for immediate actions.	Yes
M-7	Discovery Footprinting	Digital footprint should include all registered domains, sub domain sand assigned/used IP addresses with daily updates. User should be able to exclude exceptional assets like honeypots, malware sandboxes, guest networks and BYOD networks. User should be able to remove implausible items from (and add new assets to monitor to) the scorecard.	Yes
M-8	API Integration	Scans should be able to be initiated via API and the platform interface. The content returned by API should be able to include the high level data but also the details of each finding. API should allow integration with other solutions (i.e. Splunk, QRadar, etc.).	Yes
M-9	Role-based Access	Access to portal and features should be limited or expanded based on the type of role or function a user has within the system	Yes

Additional Requirements

(Preferred)

Requirement #	Feature	Description	Yes/No/Partial	Vendor's Comments
AR-1	Knowledge Base	Based on standards like NIST, MITRE (CTSA, CWRAF, CVE, CVSS, CWSS) etc. with the description and impact of the problem and remediation recommendations.	Yes	
AR-2	Compliance Check	Measure the compliance level of a company based on widely used and recognized frameworks. Pre-populated compliance report for NIST, ISO27001, GDPR with possibility to collaborate and upload & share compliance reports.	Yes	
AR-3	Financial Impact	Ability to calculate the probable financial impact if a cyber event were to occur at the Company or at a third party in order to cost-effectively achieve and maintain an acceptable level of loss exposure.	Yes	
AR-4	Technical Risk	Ability to identify technical risk in commonly assessed categories, such as Email Security, Application Security, Network Security, and Website Security.	Yes	
AR-5	Risk Scoring	Uses common frameworks to score risk (e.g., CVSS, ISO, NIST CSF) and includes measurements of * Asset Criticality (discover and classify) * Threats (events perpetrated by threat actors in the context of the critical assets and vulnerabilities) * Vulnerabilities (weaknesses in the infrastructure) * Controls (mitigating controls against the vulnerabilities) * Likelihood of a Breach (historical projected) * Impact of a Breach (business assessment based on CIA triad)	Yes	
AR-6	Multiple scan-type option	Ability to scan a vendor in order to quickly gain insight into their risk posture. Additionally, the ability to initiate a deeper scan in order to get a comprehensive look at a company's security and risk posture.	Yes	
AR-7	User Accounts	Unlimited User Access available	Yes	
AR-8	Identity and Access Management	Supports common IAM strategies	Yes	
AR-9	Robust Reporting	Ability to export all facets of the results, including technical and complaice reports. The ability to summarize reports or provide a full, in-depth reports should be available. Reporting should be both interactive and static.	Yes	
AR-10	Company Benchmarking	Ability to compare one company to one or more companies/ peers over time	Yes	
AR-11	Industry Benchmarking	Ability to compare a company's score or risk to their industry over a period of time.	Yes	
AR-12	Snapshots/Trend	Ability to easily review a company's risk posture over time with the ability to drill down into past reports for comparison	Yes	

Pricing Model *(50 words each feature) (Not Required - General descriptions are helpful)*

Feature	Description	Metric	Annual Price
Company Self Monitoring	*Describe the pricing model*		
Continuous Third Party Monitoring	*Describe the pricing model*		
Peer Reviews (benchmarking)	*Describe the pricing model*		
Merger & Acquisition targets	*Describe the pricing model*		

Business Requirements

ID #	Requirement(s)	Vendor Response	Vendor Comments *(not to exceed 75 words per requirement)*	
B-1	Is the solution cloud-based or installed on-premise?	Cloud based		General Business Requirements
B-2	Does the system provide the ability to configure workflow for onboarding without customization or assistance from vendor?	N/A		
B-3	Does the solution calculate inherent risk based on rules?	N/A		
B-4	Does the system allow for the uploading of documents provided by employees and external vendors?	N/A		
B-5	Can the solution track all correspondence between the vendor anywhere in the vendor lifecycle process/workflow?	Partial		
B-6	Describe how the system tracks fourth-party relationships.			
B-7	Please describe how historical assessments are stored and accessed.			
B-8	Does the solution provide capabilities to request more information from the vendor that may be outside the original due diligence questionnaire?			
B-9	Does the system provide capabilities to track Service-Level Agreements (SLAs)?	Yes		
B-10	Does the software send SLA metrics to vendors to document responses and attach evidence? Please describe this process.	No		
B-11	Does the solution support performance reviews sent to relationship managers?			
B-12	Is there an online/cloud portal for Vendors?	Yes		Vendor Portal
B-13	Do vendors maintain their own passwords for the portal?	Yes		
B-14	Can vendors export their questionnaire to complete offline as needed? Can completed responses be imported back into solution in an automated fashion? Please describe.	No		
B-15	Can vendors delegate or invite additional associates into the solution to assist with assessments?	N/A		
B-16	Is there a way for vendors to access a report of all open issues?	Yes		
B-17	Do vendors receive alerts of upcoming due dates, past due assignments and other actions?	No		
B-18	Can vendors provide status updates to issue resolutions?	No		
B-19	Do you allow vendors to import a completed SIG without requiring copy/paste on a question-by-question basis (one-click import)?	No		
B-20	Does the vendor have the ability to complete the questionnaire and upload/attach documents?	No		
B-21	How does the vendor see summary of questions and anything that is incomplete?	No		
B-22	Can vendors save their work and complete it at a later time/date?	No		
B-23	Can workflow be created/modified without customization or assistance from your professional services organization?	Yes		Workflow
B-24	Can the status of all workflow steps be tracked and reported on?	Yes		
B-25	Describe how workflow steps can be advanced or rejected.	Yes		
B-26	Can workflows be modified at any point in time without requiring professional services?	Yes		

Business Requirements

ID #	Requirement(s)	Vendor Response	Vendor Comments *(not to exceed 75 words per requirement)*
B-27	Will the system allow multiple departments with different access permissions to access the solution?	Yes	
B-28	Please describe how role-based access profiles are configured within the system.	Yes	
B-29	Can the solution assign alerts/notifications/tasks (systematically) to employees or vendors?	Yes	
B-30	Can our organization create questionnaires whenever needed without assistance from vendor/professional services?	No	
B-31	Can our organization incorporate/append/modify SIG content in our questionnaires?	Yes	
B-32	Does the solution provide the ability to add/create/modify risk assessment (questionnaires/templates) to include a scoring methodology?	No	
B-33	The scoring methodology must include three options: Inherent risk score = after risk assessment has been completed and before controls are in place. Critical Vendor = score based on responses from the risk assessment. Residual risk score = after risk assessment AND due diligence assessments have been completed (after controls are in place). Please describe how you support this.	No	
B-34	Does the solution provide the ability to assess the risk, by including scoring, of the vendor relationship based on the questionnaire responses?	No	
B-35	Can the system map questions back to standards, controls, risks and other business records?	No	
B-36	Does the system provide capabilities for multiple approvals based on the assessed risk score after due diligence assessments are completed by subject-matter experts (SMEs)?	No	
B-37	Does the system auto-scope questions to include for a vendor based on service or other data criteria?	No	
B-38	Does the solution securely send questionnaire(s) to the vendor via the system?	No	
B-39	Can notifications be managed/modified without professional services help (via system configuration)?	No	
B-40	Please describe how the system supports escalation emails.	No	
B-41	Does the system provide the ability to add a property/field at any point in time without requiring professional services?	No	
B-42	Can the solution be branded to include logos and company color scheme?	Yes	
B-43	Can we import data through the solution without professional services?	Yes	
B-44	Can we mass update data through solution without professional services?	Yes	
B-45	Please describe your system's ability to integrate with other systems. Please describe the level of integration possible or if there is and API available.	Yes	
B-46	Is scoring in the solution configurable? (It does not require any custom code.)	Yes	

Administration

Business Requirements

ID #	Requirement(s)	Vendor Response	Vendor Comments *(not to exceed 75 words per requirement)*	
B-46	Does the system provide canned/out-of-the-box reporting?	Yes		Reporting
B-47	Does the system provide user-configurable reporting?	Yes		
B-48	Does the system provide a dashboard view, at profile level, of activities and reporting?	Yes		
B-49	Can we produce reports in various formats such as Excel, Word, and CSV?	Yes		
B-50	Does the solution integrate with business analytics tools (such as Tableau)?	Yes		
B-51	Can we define our security rules?	Yes		Security
B-52	Is security role-based?	Yes		

Technical Requirements

ID #	Requirement(s)	Vendor Response	Vendor Comments *(not to exceed 75 words per requirement)*	
T-1	Does the system support single sign-on for all functions performed by users? (Additional logins are not required when switching between various application modules.)	Yes		General Technical Requirements
T-2	Does the solution support external role management via identity access management (IAM) automation tools?	Yes		
T-3	Does your organization publish SLAs covering availability, transaction time, storage, performance, and support requests received from the customer? (Please include Service Level Metrics with your response.)	Yes		
T-4	Do you have published minimum system requirements for any client and server software components that must be installed as part of the solution. Specs must include CPU, memory, storage throughput, and storage space. Please include these specs with your response.	Yes		
T-5	Does the solution support Internet Explorer 11 or higher for web-based components?	No		
T-6	Does the solution leverage native browser functionality? (It requires no additional plugins (Flash, Silverlight, etc.)).	No		
T-7	Do we have unlimited access to data generated by the application. Data is accessible via data exports, direct database access, or some other automated means.	Yes		
T-8	Does your organization have established windows during which any maintenance is performed?	Yes		
T-9	Does the solution include a replicated lower-level environment for development and testing activities?	Yes		
T-10	Please provide an application roadmap that includes all major system enhancements over the next 3 years.	Yes		
T-11	Does your organization publish a reference architecture that defines an ideal installation for all system components? Includes both on-premises and cloud solutions.	Yes		
T-12	Does your organization have a formalized mechanism for sending system data using SFTP? Note: Any secured protocol. Encryption is preferred.	No		
T-13	Can your organization deliver data which resides in system with a file format that is delimited by or some other customer delimiter?	No		
T-14	Are data elements well documented? Is there a data dictionary available for ease of use and integration?	Yes		
T-15	For employees, does the system support multi-factor authentication?	No		
T-16	For vendors, does the system support multi-factor authentication?	No		
T-17	Do you allow/support/enforce IP restriction, so that we can ensure that only users in our network are accessing the system (excluding the members application process)?	Yes		

SUPPLEMENTAL INFORMATION & RESOURCES

Sources Cited

a. Matthews, Greg. "Does Your Third-Party Risk Program Extend Far Enough?" KPMG LLC. Apr 2017. https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2017/04/fourth-party-risk-management.pdf.

b. Bacerra, Xavier. "California Consumer Privacy Act (CCPA)" State of California Department of Justice - Office of the Attorney General. Retrieved May 15, 2020. https://oag.ca.gov/privacy/ccpa

c. Federal Trade Commission. "Protecting Consumer Privacy and Security" Retrieved May 15, 2020. https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security

d. Proton Technologies AG. "Complete guide to GDPR compliance" Retrieved May 15, 2020. https://gdpr.eu/

e. The Committee of Sponsoring Organizations of the Treadway Commission. "Internal Control Guidance and Thought Papers" Retrieved May 15, 2020. https://www.coso.org/Pages/ic.aspx

f. Skoda Minotti Risk Advisory Services. "The SSAE 18 Audit Standard (Updates and Replaces SSAE-16)" Retrieved May 15, 2020. https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard/#

g. American Institute of Certified Public Accountants. "Attestation Standards: Clarification and Recodification" Retrieved May 15, 2020. https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf

h. U.S. Department of Commerce. "NIST Cybersecurity Framework" Retrieved May 15, 2020. https://www.nist.gov/cyberframework

i. Center for Internet Security. "Cybersecurity Best Practices" Retrieved May 15, 2020. https://www.cisecurity.org/cybersecurity-best-practices/

j. Office of the Under Secretary of Defense for Acquisition & Sustainment. "Cybersecurity Maturity Model Certification" Retrieved May 15, 2020. https://www.acq.osd.mil/cmmc/

k. Whistic. "5 of the Top Questionnaires for IT Vendor Assessments" Retrieved May 15, 2020. https://blog.whistic.com/5-of-the-top-questionnaires-for-it-vendor-assessments-e1fc5b927eb9

l. Mike Davis. "Cyber Security Risk, what does a 'reasonable' posture entail, and who says so?" Retrieved May 15, 2020. https://alliantcybersecurity.com/cybersecurity-risk-reasonable-posture/

SUPPLEMENTAL INFORMATION & RESOURCES

m. FAIR Institute. "Targeting Cybersecurity Investment - a FAIR Approach" June 24, 2019. Retrieved May 15, 2020.
https://www.fairinstitute.org/blog/targeting-cybersecurity-investment-the-fair-approach

n. U.S. Chamber of Commerce. "Principles for Fair and Accurate Security Ratings" June 20, 2017. Retrieved May 15, 2020. https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

o. FAIR Institute. "Quantification: the Core of Effective Cyber Risk Management" Retrieved May 15, 2020. https://www.fairinstitute.org/fair-risk-management

p. U. S. Department of Commerce. "Common Vulnerability Scoring System (CVSS)" Retrieved May 15, 2020. https://nvd.nist.gov/vuln-metrics/cvss

q. Ponemon Institute LLC. "The Cost of Third-Party Cyber Risk Management" March 2019. Retrieved May 15, 2020.
https://cdn2.hubspot.net/hubfs/2378677/Content-Assets/CyberGRX%20Ponemon%20Report.pdf

r. Cyentia Institute. "Ripples across the risk surface" March 2019. Sponsored by Risk Recon. Retrieved May 15, 2020. https://cdn2.hubspot.net/hubfs/2477095/Ripples%20Across%20the%20Risk%20Surface%20report%20-%20Nov%202019.pdf

Other References

s. Federal Trade Commission. "The Financial Services Modernization Act (Gramm Leach Bliley Act (GLBA)" https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

t. Federal Financial Institutions Examination Council (FFIEC). https://www.ffiec.gov/

u. Legal Information Institute. 18 U.S. Code Chapter 121—Stored wire and electronic communications and transactional records access - Stored Communications Act ("SCA").
https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

v. Legal Information Institute. 18 U.S. Code Chapter 119—Wire and electronic communications interception and interception of oral communications - Electronic Communications and Privacy Act ("ECPA") https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

w. Legal Information Institute. "18 U.S. Code Chapter 1030—Fraud and related activity in connection with computers - Computer Fraud and Abuse Act ("CFAA"). https://www.law.cornell.edu/uscode/text/18/1030

SUPPLEMENTAL INFORMATION & RESOURCES

x. Attorney General of Texas. Texas Business & Commerce Code ("TBCC")
https://statutes.capitol.texas.gov/Docs/SDocs/BUSINESSANDCOMMERCECODE.pdf

y. Attorney General of Texas. Texas' Identity Theft Enforcement and Protection Act ("ITEPA")
https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm

z. Gartner. "Effectively Mitigate Third-Party Risk. Shift from a point-in-time to an iterative approach to manage new third-party risks" https://www.gartner.com/en/legal-compliance/trends/third-party-risk

aa. U.S. Department of Commerce. "Assessment & Auditing Resources".
https://www.nist.gov/cyberframework/assessment-auditing-resources

List of the example TPRM getting started artifacts

a. TPRM Policy Template https://cisosconnect.com/media_center/folders/91896/files/234197/download

b. RFI for CISOs Template https://cisosconnect.com/media_center/folders/91896/files/234198/download

c. Example Contract Clauses for data security and privacy
https://cisosconnect.com/media_center/folders/91896/files/234196/download

d. Third Party Risk Management survey SIG
https://cisosconnect.com/media_center/folders/91896/files/234195/download

security current cisos connect

Security Current and CISOs Connect cybersecurity knowledge-sharing community provide CISOs with the opportunity to share knowledge and collaborate with CISOs globally.

Overseen by a CISO editorial board from a broad range of industries, Security Current and CISOs Connect offer peer-researched content and events designed to help CISOs navigate the complex and challenging field of cybersecurity.

Security Current and CISOs Connect features podcasts and webinars, CISO-generated research reports, insights, CISO and vendor profiles, as well as practical advise.

Security Current and the CISOs Connect community facilitate CISO to CISO knowledge sharing of real-world experiences on security, risk management and governance challenges. CISOs Connect is the only platform that allows fully-vetted CISOs to spark and facilitate discussions on cybersecurity issues with other leading CISOs all over the world.

Timely. Original. Strategic: Security Current/CISOs Connect is an important weapon in the arsenal of every CISO.