THIRD-PARTY SECURITY

RISK MANAGEMENT PLAYBOOK

A study of common, emerging, and pioneering capabilities and practices

riskrecon

mastercard

A study sponsored by RiskRecon, Inc. | WWW.RISKRECON.COM

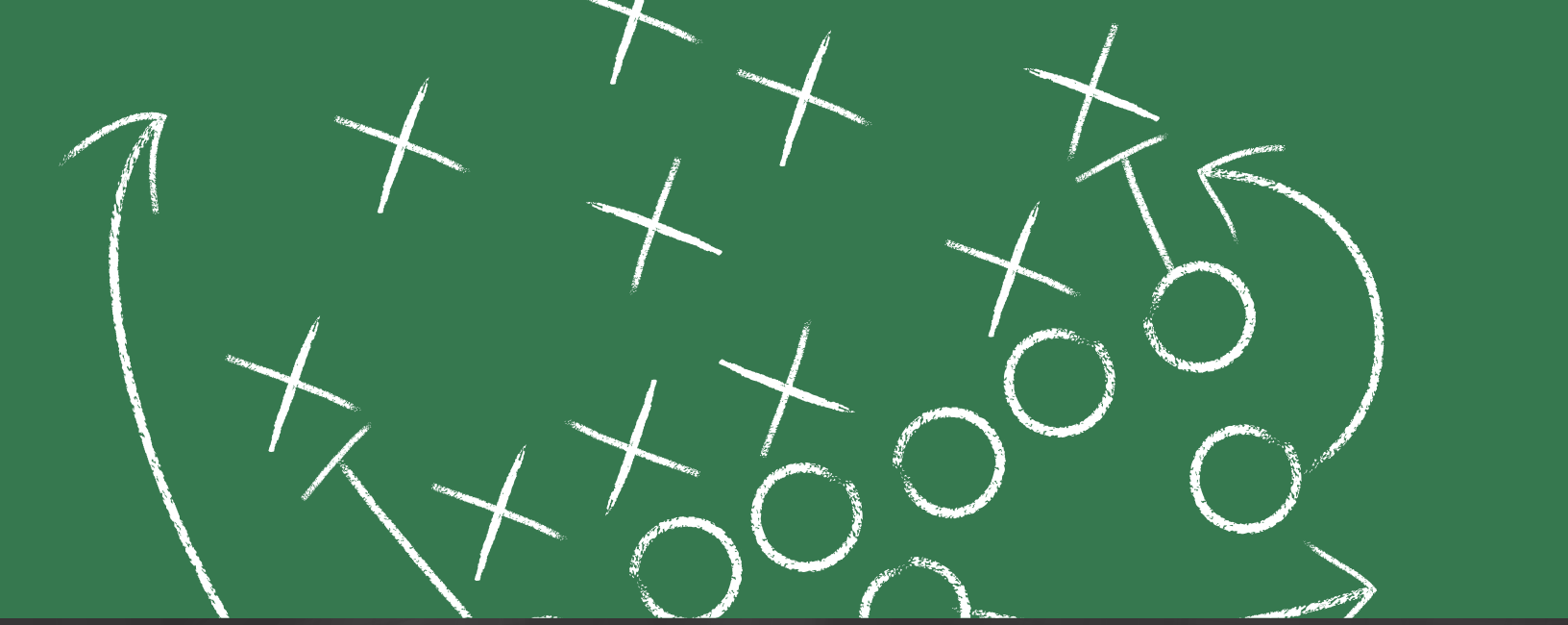


TABLE OF CONTENTS

OVERVIEW

EXECUTIVE SUMMARY

The *Third-Party Security Risk Management Playbook* (*Playbook*) is the definitive study of third-party security risk management practices. Based on in-depth interviews of risk executives from 30 domestic and global firms, it reveals the real-world capabilities and practices employed to manage third-party cyber risk, distilled into 14 capabilities with 72 common, emerging, and pioneering practices.

Compare your own program with the *Playbook* data about what other organizations are doing. Use it to identify your own goals and objectives and refer to the Playbook to determine which capabilities and practices make sense for you.

The *Playbook* data show that there is a common set of widely adopted third-party risk management practices, founded on strong program management practices and and periodic risk assessments rooted in questionnaire-based information collection and analysis. However, innovative organizations are aggressively breaking out of the traditional periodic attestation-centric model, developing capabilities to gain *continuous* insight into third-party risk and act on that information. They are seeing promising results from their early efforts in these areas, reporting better risk outcomes and better scale.

The *Playbook* focuses on capabilities and practices unique and interesting to third-party risk management. Common business management practices such as budgeting and staffing, while prerequisite to the success of third-party risk management, are intentionally excluded.

ACKNOWLEDGEMENTS

Thank you to the executives from 30 enterprises leading third-party risk management initiatives who shared their program practices and expert insight to provide this *Playbook*. They each joined in third-party risk round table discussions, participated in formal interviews, and reviewed drafts to bring this study to publication.

WHY THIRD-PARTY RISK MATTERS

BIG IMPACT

Enterprises entrust the protection of their crown jewels—their customer data, their reputation, their finances, and their business availability—with third parties. A breach of your third party is a breach of your enterprise, so you need to know: Are they trustworthy? Why? Why not? What should be done about it? These questions are yours to answer and act on.

BIG CHALLENGES

Third-party risk management is hard. It requires deep transparency, strong accountability, and effective collaboration. Third-party risk has to achieve this position with hundreds and even thousands of organizations while being an outsider to every organization. Additionally, third-party risk has to solve this with limited personnel and resources.

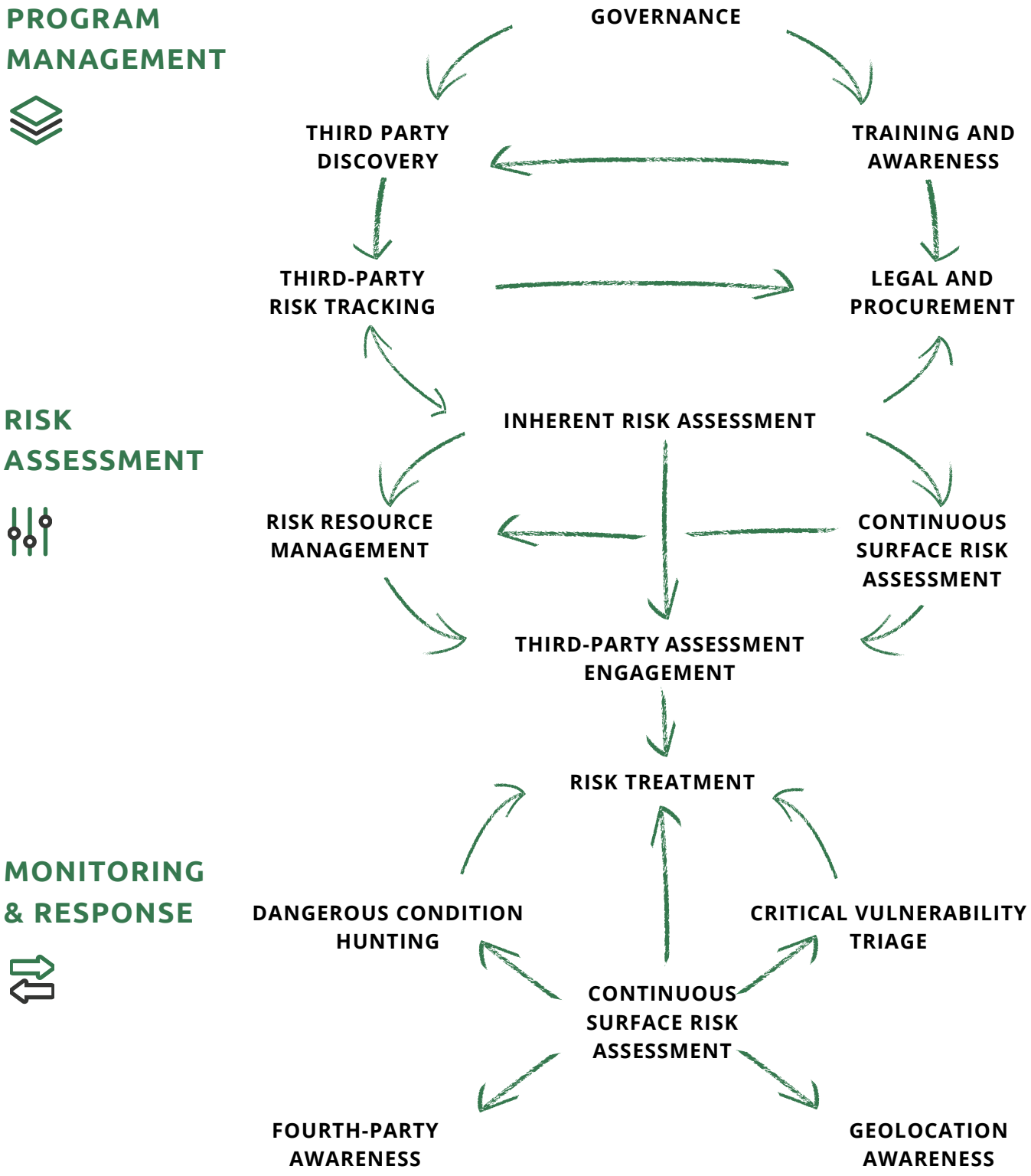
This need—to achieve really good risk outcomes from the outside with limited resources—will result in dramatic risk management innovation, key of which will be development of machine learning and artificial intelligence-based risk assessment capabilities. These inventions will occur within the context of third-party risk management and be adopted by enterprises for internal risk management. Necessity is the mother of invention, and the necessity is pressing in a big way.

THE GREATER GOOD

Third-party risk management is a process of holding enterprises accountable to good risk management practices. As you improve the risk management capabilities of your third parties you improve the security of the Internet. The improvement decreases the likelihood of data being breached, decreases the likelihood of systems being turned into DDOS drones or malware servers, and increases the likelihood that systems are going to reliably fulfill their intended purposes. The work of third-party risk management is work for the greater good.

PLAYBOOK STRUCTURE

The Playbook is organized as a set of 14 capabilities containing a total of 72 practices. The capabilities are divided into three domains.

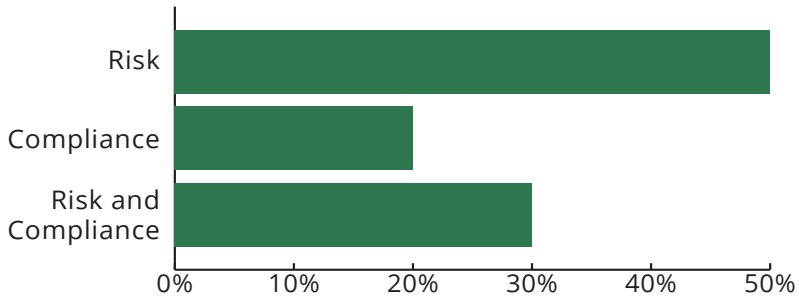


SUMMARY

Participant Count

Finance / Insurance	12
Healthcare	7
Manufacturing	6
Technology	5
Total Companies	**30**

Primary Program Motive



"We spun up our third-party security risk program shortly after the FBI informed us that our data was for sale on the dark web. We traced the breach back to one of our vendors."

- A Regional Healthcare Provider

SUMMARY OF OBSERVATIONS

PARTICIPANT DEMOGRAPHICS

What percentage of vendors require on-going cyber risk management?

The healthcare industry has the highest percentage of their total vendor population that require ongoing cyber security risk management at 19%, followed by finance / insurance at 13%.

You might want to double check your risk calculations if you are in healthcare or finance and are only managing cyber security risk of 3% of your vendors.

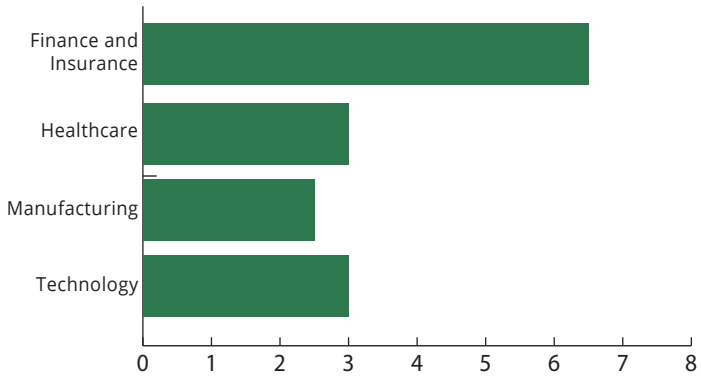
	Average
Finance / Insurance	13%
Healthcare	19%
Manufacturing	2%
Technology	7%

11.7%

Overall average

Who has the most experience operating third-party risk management programs?

Look to the financial sector for wisdom in managing third-party cyber risk. They have been operating their programs for an average of 6.5 five years.



Where does your third-party security risk team report into?

97% of third-party security risk teams report into Information Security.

Organizational expertise and mission focus were the primary reasons reported for having the function report into information security.

How many risk rating tiers do you use?

It is pretty common to see firms use four or five risk rating tiers. The reason? Many companies have created a 'critical' tier as a home for those vendors that are absolutely essential to the success of the organization.

5 tiers used	33%
4 tiers used	33%
3 tiers used	28%
2 tiers used	6%

PROGRAM OPERATIONS INSIGHTS

How many security risk analysts does it take to manage a vendor?

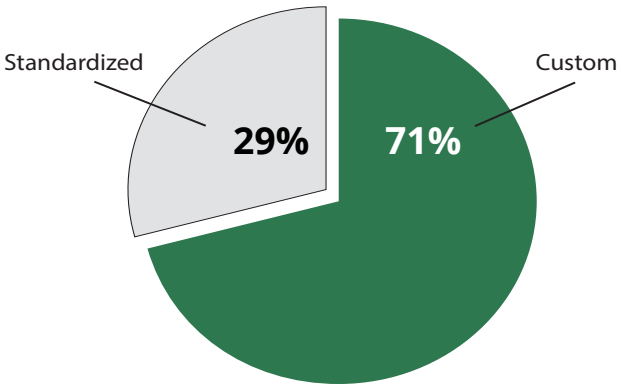
Well, it depends on the industry. The financial sector allocates more analyts per vendor than any other sector, with one analyst handling the recurring assessment load of 73 vendors. You get into the other sectors and it can be as high as one analyst managing 133 vendors.

Is there an inverse relationship between regulatory oversight load and analyst management load? Perhaps, though more data is required to answer this question.

	Low	High	Average
Finance / Insurance	20	150	73
Healthcare	40	125	93
Manufacturing	32	175	102
Technology	67	200	133

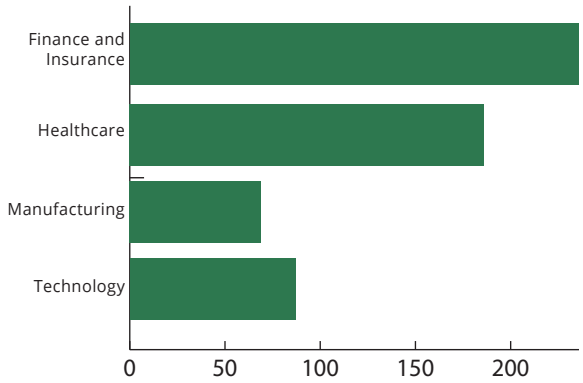
Can't we all just agree on a standard questionnaire?

No. Seventy-one percent of companies are still using a custom questionnaire. Interestingly, the vast majority of firms using a standardized questionnaire are in the healthcare sector. The financial sector hasn't yet solidified around a common questionnaire. No standardization there.



Wow! That is a lot of questions!

Expect to get a questionnaire containing 280 questions if you are a vendor to a financial services company. The manufacturing and technology sectors ask less than 100 questions.



SUMMARY OF OBSERVATIONS

CAPABILITIES: PROGRAM MANAGEMENT

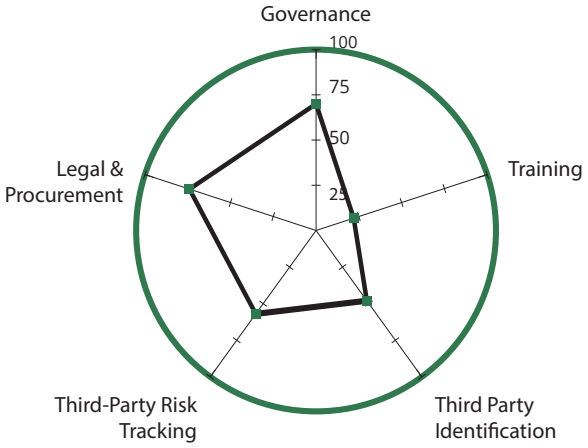
Common Practices

- **Governance** - Policies state the intended third-party risk outcomes. Standards and operating procedures provide the framework within which the policy objectives are accomplished.
- **Training** - Internal stakeholders are trained in their third-party risk management responsibilities.
- **Discovery** - Third-party risk management is integrated with the procurement and contracting processes. Periodically review the vendor database for new vendors.
- **Tracking** - Third parties are tracked in a central database.
- **Legal & Procurement** - Third parties are contractually committed to meeting security requirements and grant the right to audit. Exceptions require executive approval.

Emerging Practices

- **Governance** - Third-party security risk management program risk outcomes are measured and reported.
- **Discovery** - Unmanaged third parties are discovered through analysis of web activity logs.
- **Tracking** - Risk issues are tracked in a formal risk registry.
- **Legal & Procurement** - Require that existing vendors address material issues before renewing or expanding the contract.

Capability Practice Adoption



Pioneering Practices

- **Training** - Provide third parties training on your security requirements. Host vendor security awareness events and seminars.
- **Discovery** - Build relationships with business owners to identify opportunities to support new and existing vendor relationships.

SUMMARY OF OBSERVATIONS

CAPABILITIES: RISK ASSESSMENT

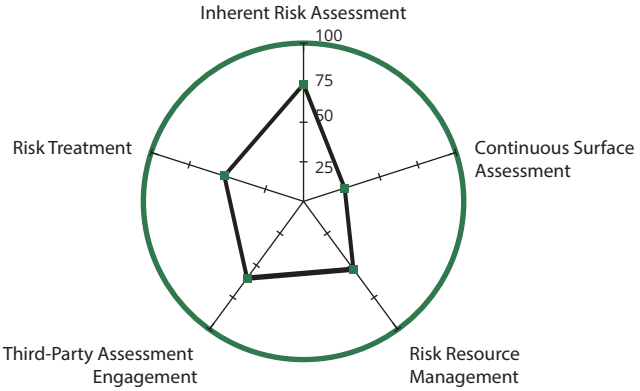
Common Practices

- **Inherent Risk Assessment** - Implement a framework for assessing third-party inherent risk. Assign each vendor an inherent risk rating.
- **Risk Resource Management** - Set third-party assessment frequency and scope based on inherent risk rating.
- **Third-Party Assessment Engagement** - Conduct third-party assessments according to established standards. Discuss status of open issues from previous assessments.
- **Risk Treatment** - Share the assessment results with the vendor and internal stakeholders. Hold vendor accountable to addressing issues. Record assessment results in a risk register.

Emerging Practices

- **Continuous Surface Assessment** - Maintain current understanding of third-party exposure by continuously assessing third-party surface risk conditions.
- **Risk Resource Management** - Determine assessment frequency based on residual risk, factoring inherent risk rating with prior assessments or continuous assessment results.

Capability Practice Adoption



Pioneering Practices

- **Third-Party Assessment Engagement** - Adjust the assessment plan based on the continuous surface assessment results.
- **Risk Treatment** - Use continuous surface security assessment capability to monitor areas of concern for improvement. Provide third parties on-going access to continuous surface assessment results for their own organization.

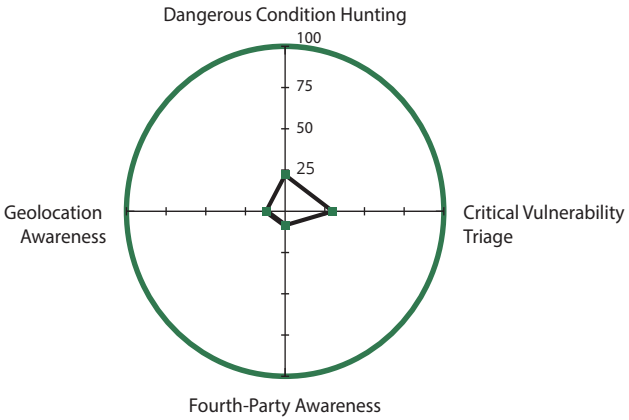
SUMMARY OF OBSERVATIONS

CAPABILITIES: MONITORING & RESPONSE

Emerging Practices

- **Dangerous Condition Hunting** - Systematically monitor third parties for security events such as data breach and security compromise. Define reponse procedures for handling third-party breach events.
- **Critical Vulnerability Triage** - Provide third parties risk advisories regarding critical vulnerabilities. Maintain awareness of software operating in the surface systems of third parties through the continuous surface security assessment capability.

Capability Practice Adoption



Pioneering Practices

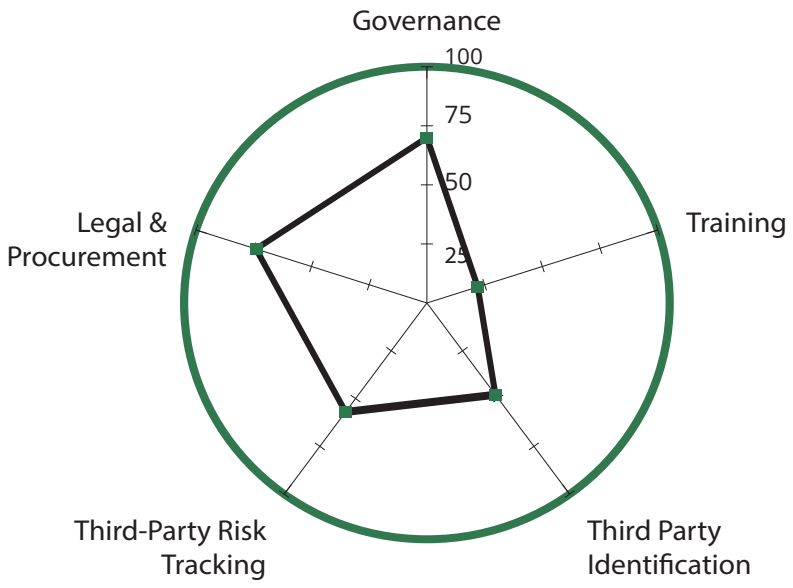
- **Dangerous Condition Hunting** - Maintain a list of dangerous conditions that are specifically not allowed to be present in third-party environments. Frequently analyze the results of continuous surface risk assessments to discover dangerous security conditions. Tactically engage third parties to address dangerous security conditions.
- **Critical Vulnerability Triage** - Escalate the priority of third parties known to be exposed to the critical vulnerability based on continuous surface security assessment data.
- **Fourth-Party Awareness** - Know third-party portfolio service providers - your fourth parties. Monitor significant fourth parties for material security breaches and operational outages. Develop and enforce control assessment standards for assessing third-party use of significant fourth parties.
- **Geolocation Awareness** - Know third-party system geo-locations. Monitor for illegal or risky geographies, which may shift over time due to regulations, geopolitical tensions or natural disasters.

DETAILS

PROGRAM MANAGEMENT

Governance	Formally charter the third-party risk management program and give it teeth through policies and standards. Measure and report program outcomes.
Training and Awareness	Promote the third-party risk program, informing stakeholders of relevant policies, standards, and operating procedures. Keep third parties informed of performance requirements.
Third Party Identification	Implement processes to identify third parties. Engage the third-party risk management team through all relationship stages – evaluation, onboarding, operation, modification, and termination.
Third-Party Risk Tracking	Track third-party risk in a central database where the third-party risk profile, assessment results, and open issues are managed.
Legal and Procurement	Contractually enforce third-party security performance requirements and the right to audit. Leverage purchasing events to force closure of open third-party issues.

Average Capability Practice Adoption Rate



CAPABILITY

GOVERNANCE

WHAT

Establish policies that state the intended third-party risk outcomes. Implement standards and operating procedures to provide the framework within which the policy objectives are accomplished.

WHY

Policies formally commit the organization to the stated risk objectives. Standards and operating procedures are necessary to make good on the commitments. From these, follow investments in related people, process, and technology.

HOW

Create third-party risk management policies and related standards in collaboration with key stakeholders and executive management. It will likely be necessary to lay the groundwork of educating decision makers on the value of third-party risk management. In discussing policy options, be transparent about the benefits, limitations, and costs.

PRACTICE	STATUS	ADOPTION
Policies are established that state the intended third-party risk outcomes.	Common	90%
Standards set the criteria against which third-party security risk is evaluated.	Common	87%
Procedures are implemented for measuring third-party inherent risk.	Common	77%
Procedures are implemented for assessing third-party risk performance.	Common	77%
Assessment procedures account for differences in third-party inherent risk.	Common	60%
The third-party risk program is formally integrated with essential partners in the organization, such as purchasing, legal, and compliance.	Common	77%
Program activities are measured and reported.	Common	60%
Program risk outcomes are measured and reported.	Emerging	37%

"Our biggest challenge is finding people who can successfully walk the cyber security dog through the vendor technical evaluations and the executive-level discussions."

- Regional Healthcare Company

CAPABILITY

TRAINING AND AWARENESS

WHAT

Educate internal stakeholders about third-party risk and their responsibilities in ensuring it is properly managed. Inform third parties of their obligations during the on-boarding process and periodically going forward.

WHY

Training internal stakeholders helps ensure the program is successfully integrated into their operations. Keeping third parties aware of your risk management expectations enables them to proactively address potential gaps.

HOW

Create a third-party risk management training program that informs stakeholders of their role-specific responsibilities and motivates their participation.

Provide third parties periodic updates of security performance expectations. Meet periodically with critical third parties for one-on-one risk collaboration.

PRACTICE	STATUS	ADOPTION
Provide internal stakeholders with third-party security risk awareness and management process training.	Common	67%
Train third parties on your vendor security requirements.	Pioneering	23%
Require that third-party personnel with sensitive access to your assets individually take your security awareness and policy training.	Pioneering	7%
Meet periodically with the most critical vendors to openly discuss current and emerging security concerns.	Pioneering	7%
Periodically host general security awareness events for your third-party community.	Pioneering	7%

"How do you share information with vendors without being their security standard? We don't want them to abdicate their responsibility for protecting their systems."

- Global Financial Institution

CAPABILITY

THIRD PARTY IDENTIFICATION

WHAT

Implement processes to identify new third parties and changes to existing third parties.

WHY

You can't manage what you don't know. Identifying new third parties and changes to existing third parties enables you to engage your risk processes.

HOW

If you are starting a new program, analyze the vendors in the procurement database to create your initial population. Then periodically analyze the procurement database to identify venders that were missed.

Tie into the procurement processes to engage new vendors. Hook in to the project management program and business owners to identify new third parties early and existing ones that you missed.

PRACTICE	STATUS	ADOPTION
Seed your program with active vendor records in the procurement database.	Common	70%
Implement explicit procurement process gates to be included in contracting with new third parties.	Common	73%
Implement explicit procurement process gates to be engaged in material changes to existing vendor relationships.	Common	73%
Implement explicit IT process gates to be involved in projects that require new third parties or changes to existing third parties.	Emerging	37%
Build relationships with business owners to identify opportunities to support their new and existing third-party relationship needs.	Pioneering	13%
Periodically analyze the procurement vendor database to identify third parties that aren't already under management.	Common	60%
Analyze network traffic logs / web activity to identify identify unmanaged third parties.	Emerging	30%

"We get a monthly report of new vendors added to the accounts payable system and review those for any vendors that we may have missed."

- National Health Insurance Company

CAPABILITY

THIRD-PARTY RISK TRACKING

WHAT

Centrally document third parties and their risk attributes. Document the results of assessments and track issues in a risk registry.

WHY

Tracking third-party risk, including their inherent risks and business context, is a pre-requisite to managing third-party risk. Tracking of issues is necessary to understand third-party residual risk and to resolve issues.

HOW

Track vendors, their risk attributes, business context, and issues in a central system. The system should support analysis and reporting.

PRACTICE	STATUS	ADOPTION
Maintain procurement records that can be readily analyzed.	Common	70%
Track third-party risk in a central database.	Common	50%
Track third-party issues in a risk registry.	Common	50%
Track third-party residual risk, factoring inherent risk rating with assessment performance.	No Data	No Data

"You can't manage third-party risk if you can't track your third parties."

- National Insurance Provider

CAPABILITY

LEGAL AND PROCUREMENT

WHAT

Contractually enforce third-party security performance requirements and the right to audit. Require notification of any material security breach. Leverage purchasing events to motivate closure of open issues.

WHY

Contractual obligations motivate third parties to have at least a basic risk management program. It also gives you a basis of transparency and accountability to hold them to performance obligations.

Issuance of new purchase contracts can be a strong leverage point to motivate third parties to address outstanding issues.

HOW

Develop template contract language that establishes risk performance requirements. Include these terms in contracts where inherent risk requires it. Don't allow exceptions without serious consideration and formal risk acceptance by executive management.

Use purchasing events as leverage to get third parties to address open issues.

PRACTICE	STATUS	ADOPTION
Contractually commit third parties to meet your security risk performance requirements.	Common	90%
Contractually obligate third parties to allow you to audit their security risk performance.	Common	90%
Contractually obligate third parties to provide timely notification of material data breaches and other security events.	Common	90%
Require executive approval for exceptions to contractual risk management terms.	Common	73%
Require that new vendors address material issues prior to awarding the purchase order.	Common	53%
Require that existing vendors address material open issues prior to expanding the contract or issuing a new purchase order.	Emerging	27%

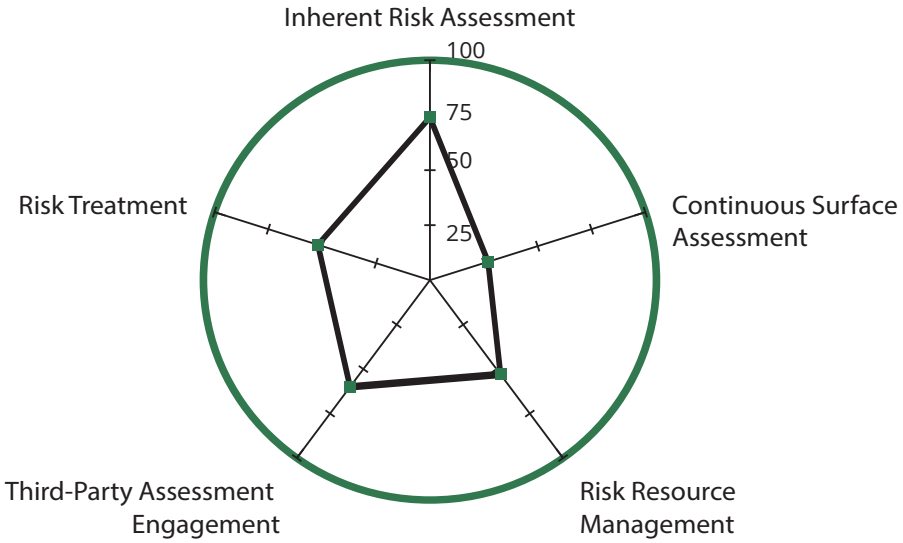
"If a vendor does not agree to our contractual terms we track it as an issue in our risk registry. It wins them a spot on our watch list."

- Credit Card Issuer

RISK ASSESSMENT

Inherent Risk Assessment	Know the inherent security risks of each third-party relationship.
Continuous Surface RIsk Assessment	Maintain current understanding of third-party exposure by continuously assessing third-party surface risk conditions.
Risk Resource Management	Allocate risk resources to match third-party residual risk exposure. Conduct assessments of low-performing third parties more frequently and at greater depth. Conduct assessments less frequently for high performing third parties.
Third-Party Assessment Engagement	Periodically conduct an assessment engagement of each third party to gain privileged visibility to the risk management program. Tune the assessment plan based on third-party inherent risk and known strengths and weaknesses.
Risk Treatment	Engage with the third party to address risk performance gaps in a timely manner.

Average Capability Practice Adoption Rate



CAPABILITY

INHERENT RISK ASSESSMENT

WHAT

Know the inherent risks of doing business with each third party. Understand the assets at risk and potential negative outcomes of a security failure.

WHY

Knowledge of third-party inherent risks enables you to understand what is at stake with each entity and informs what risks should be managed and to what degree.

HOW

Assign each third party an inherent risk rating using a consistent framework with enough inherent risk tiers to meaningfully segment the portfolio. Differentiate inherent risk tiers based on attributes such as assets and services exposed, connectivity, and so forth.

PRACTICE	STATUS	ADOPTION
Implement a framework for assessing third-party inherent risk.	Common	87%
Implement a simple criteria in the procurement process for purchasing agents to use to identify vendors that require professional risk assessment.	Common	77%
Assign each third party an inherent risk rating.	Common	77%
Document inherent risk attributes such as services, data types, transaction types, and connectivity.	Common	77%
Periodically review third-party relationships for material changes to inherent risk.	Common	53%

"If the vendor has any of our customer data then we just assume they have all of it because scope always creeps."

- Health Insurance Company

CAPABILITY

CONTINUOUS SURFACE RISK ASSESSMENT

WHAT

Maintain current understanding of third-party exposure by continuously assessing third-party surface risk conditions.

WHY

Attestation-based assessments tell you what investments companies have made in risk management. Continuous surface security assessment data objectively tells you how well they implement and operate their program.

It enables you to know the internet IT profile of your third parties, provides objective measurement of security risk performance, and enables rapid identification and triage of dangerous conditions. It facilitates smarter engagements that target areas of known weakness, while deemphasizing areas of known strength.

HOW

Implement capabilities to continuously discover vendor internet-facing assets and to collect relevant system security measurements and related intelligence such as data-loss events, IP reputation, and threat intelligence activity. Build capability to analyze results to measure third-party performance and identify dangerous conditions and events. Implement event-based risk alerting to efficiently identify third-party conditions that require attention.

PRACTICE	STATUS	ADOPTION
Maintain current knowledge of third-party Internet surface IT profile, including domains, networks, systems, system hosting providers, and system geo-locations.	Emerging	27%
Maintain current knowledge of third-party Internet suface software and system security configurations.	Emerging	27%
Systematically monitor threat intelligence feeds and data breach alert channels and correlate the data with your third-party surface IT profile.	Emerging	27%
Maintain a continuous risk performance profile of each third party by continuously analyzing the data from the Internet IT profile, surface security configuration, and the threat intelligence feeds.	Emerging	27%

"Attestation tells us what risk management practices the vendor has implemented. Continuous surface risk assessments tell how well they execute on those practices."

- Global Financial Institution

CAPABILITY

RISK RESOURCE MANAGEMENT

WHAT

Allocate risk assessment resources commensurate with the residual third-party risk exposure, informed by inherent risk, results from previous assessments, and data from continuous surface risk assessments.

WHY

Allocating resources based on residual exposure improves outcomes by focusing analyst attention on improving performance of poor performing third parties. It yields better scale because analysts are not wasting time over-assessing third parties that are strong performers.

HOW

Allocate resources based on residual risk rather than inherent risk. Calculate residual risk by factoring inherent risk with results from previous assessment engagements and continuous surface assessment results. Increase assessment frequency and depth for poorly performing third parties. Decrease assessment frequency and scope for strong performers. For example, you might set a schedule as shown below:

	Assessment Frequency	
Inherent Risk Rating	Weak Performance	Strong Performance
Critical	12 months	18 months
High	12 months	24 months
Medium	24 months	36 months

PRACTICE	STATUS	ADOPTION
Determine assessment frequency based on inherent risk rating.	**Common**	**70%**
Determine assessment frequency based on residual risk rating, factoring inherent risk rating with prior assessment or continuous surface assessment results.	**Pioneering**	**23%**
Establish baseline control assessment scope and validation requirements commensurate with each risk rating.	**Common**	**77%**
Modify assessment control scope to match the predominant architecture patterns (on-premise, cloud, and so forth).	**Emerging**	**43%**

"We set assessment frequency based on residual risk. Why assess strong performers at the same frequency of low performers?"

- Regional Healthcare Company

CAPABILITY

THIRD-PARTY ASSESSMENT ENGAGEMENT

WHAT

Periodically execute a privileged-access assessment of each third party. Tune the assessment plan based on third-party inherent risk and known strengths and weaknesses.

WHY

Privileged-access assessments provide a comprehensive understanding of the security risk management program from which you can best measure risk exposure and prescribe recommendations for tactical and systemic performance improvement.

HOW

Prepare for the assessment by reviewing prior assessments and continuous surface assessment data. Familiarize yourself with the organization's IT profile, including hosting providers, hosting geo-locations, and technology stack. Modify the assessment plan to go deep into areas of control weakness and back off on areas of strength.

Use the third party representations to understand how they have invested in risk-management people, processes, and technology. Use the objective continuous surface assessment data to inform you of how well they have implemented and are operating their risk management program. Also, use the surface assessment data to validate third-party claims, calling out technical gaps and identifying root cause issues.

PRACTICE	STATUS	ADOPTION
Conduct third-party enterprise assessments according to established standards and methodology.	Common	90%
Discuss the status of open issues from previous assessments with the third party.	Common	80%
Adjust the assessment plan based on the results of prior third-party assessment engagements.	Common	53%
Adjust the assessment plan based on the continuous surface assessment results.	Pioneering	17%

"It is very rare that a vendor allows us to do an on-site visit anymore."

- Global Credit Card Issuer

CAPABILITY

RISK TREATMENT

WHAT

Engage with third parties to address tactical and systemic security performance gaps necessary to achieve a satisfactory risk-management position.

WHY

Reduce your risk exposure by holding your third parties accountable to meeting your risk management performance standards. Customer risk feedback to vendors that is timely, relevant, and actionable is a powerful motivator for third parties to do the right thing.

HOW

Provide your third parties with risk-prioritized action plans that guide them in addressing tactical and systemic risk. Set expectations for issue remediation timing and follow up on all commitments. Proper risk prioritization is essential to ensure that resources are deployed first to issues that matter most and only to issues that actually expose you to risk.

For more proactive engagement with your third parties, provide them access to continuous surface risk assessment results. With access to continuous surface assessment results, third parties can proactively address issues that you would otherwise have to communicate.

PRACTICE	STATUS	ADOPTION
Share the assessment results with the third party.	Common	87%
Share the assessment results with internal stakeholders.	Common	80%
Record assessment results in a risk register.	Common	53%
Hold third parties accountable to addressing the identified issues.	Common	60%
Provide third parties ongoing access to continuous surface assessment results for their own organization.	Pioneering	10%
Use a continuous surface security assessment capability to monitor areas of concern for improvement.	Pioneering	23%

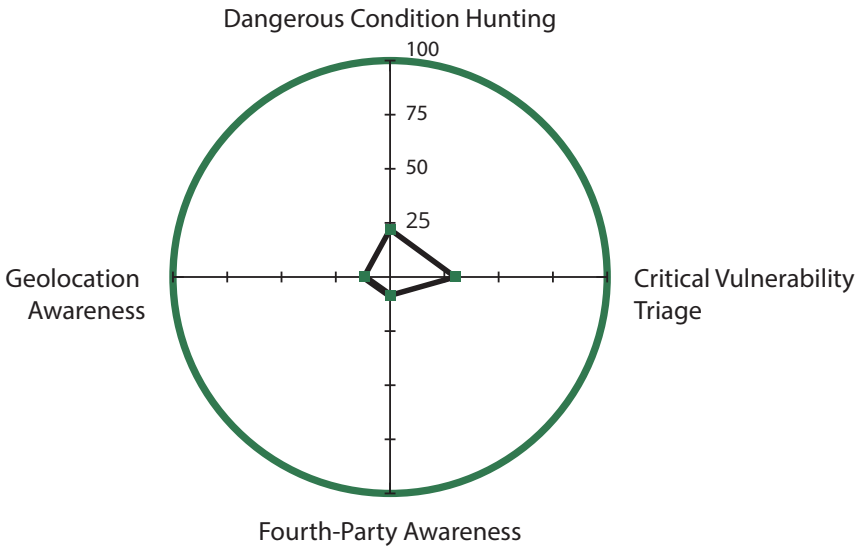
"We put poor performing vendors on a watch list. Stay there too long and you will land on our 'do not do business with' list."

- Global Financial Institution

MONITORING & RESPONSE

Dangerous Condition Hunting and Response	Rapidly discover and act on third-party security events and material control failure conditions.
Critical Vulnerability Triage	Critical vulnerability exposures to fast-moving threats across the third-party portfolio are immediately known and mitigated.
Fourth-Party Awareness	Know third-party portfolio service provider dependencies -- your fourth parties. Maintain at least a high level risk awareness of significant fourth parties where you have third-party portfolio concentration risk.
Geo-Location Awareness	Know third-party system geolocations. Monitor for illegal or risky geographies, which may shift from time-to-time due to regulations, geopolitical tensions or natural disasters.

Average Capability Practice Adoption Rate



CAPABILITY

DANGEROUS CONDITION HUNTING AND RESPONSE

WHAT

Rapidly detect and act on material third-party security events and dangerous control conditions.

WHY

Minimize damage caused by third-party security incidents such as data loss, compromise, and system outage. Prevent dangerous control conditions from resulting in security incidents.

HOW

This capability is facilitated through implementation of the continuous surface risk assessment capability.

Monitor public and deep-channel sources for early insight into impactful events and initiate vendor incident response processes upon detection. Frequently analyze third-party surface security posture to identify dangerous conditions. Tactically engage third parties to address dangerous conditions, providing context to facilitate rapid remediation.

PRACTICE	STATUS	ADOPTION
Define response procedures for handling third-party breach events.	Emerging	47%
Systematically monitor third parties for security events such as data breaches and security compromises.	Emerging	30%
Formally maintain a list of 'dangerous' conditions that are specifically not allowed to be present in third-party environments. For example, the list might include Windows NT or WordPress 2.1.	Pioneering	7%
Frequently monitor the results of continuous surface risk assessments to discover dangerous security conditions.	Pioneering	13%
Tactically engage third parties to triage dangerous security conditions and pressing performance concerns.	Pioneering	13%

"We are getting huge returns on our dangerous condition hunting program. We get rapid risk reduction and it raises awareness with vendors."

- Global Financial Institution

CAPABILITY

CRITICAL VULNERABILITY TRIAGE

WHAT

Rapidly pinpoint and triage exposure to critical vulnerabilities in third-party systems.

WHY

Rapid triage of third-party exposure to critical vulnerabilities reduces likelihood of harm.

HOW

Faciliate this capability by implementing the continuous surface risk assessment capability.

Maintain current knowledge of the software operating on third-party systems. When a critical vulnerability emerges, query the third-party software inventory for systems running the vulnerable software. Prioritize triage efforts towards third parties known to be exposed to the critical vulnerability.

PRACTICE	STATUS	ADOPTION
Provide third parties risk advisories regarding critical vulnerabilities.	Emerging	40%
Survey vendors to understand their exposure to critical vulnerabilities and understand their related mitigation action plans.	Emerging	36%
Maintain awareness of the software operating in the surface systems of third parties through the continuous surface security assessment capability.	Emerging	27%
Prioritize triage efforts towards third parties known to be exposed to the critical vulnerability.	Pioneering	17%
Share system vulnerability data with your third parties to assist them in remediation.	Pioneering	10%
Monitor third-party remediation of critical vulnerabilities through the continuous surface security assessment capability.	Pioneering	17%

"It is very dangerous to assume that all vendors are taking critical vulnerabilities seriously. We send out critical vulnerability risk advisories to our third parties to ensure a base level of awareness across our supply chain."

- Global Media Company

CAPABILITY

FOURTH PARTY AWARENESS

WHAT

Know third-party portfolio service providers - your fourth parties. Maintain at least a high level risk awareness of significant fourth parties where you have third-party portfolio concentration risk.

WHY

Mapping service providers to your third parties enables you to understand your service provider concentration risk. If Dynamic Network Services or AWS Ireland goes down, which of my third parties are impacted?

Identifying significant fourth parties also enables you to develop control assessment standards for assessing third-party use of significant providers.

HOW

Faciliate this capability by implementing the continuous surface risk assessment capability.

Identify the hosting providers of third-party systems using network registration information associated with each third-party system IP address. Monitor significant fourth parties for security breaches and service outages that may impact your third parties.

Develop and enforce control assessment standards for assessing third party use of significant fourth parties. Faciliate conducting expansive assessment of significant fourth parties in cases where the fourth party is also your third party.

PRACTICE	STATUS	ADOPTION
Know the service providers used by your third parties.	Pioneering	17%
Monitor significant fourth parties for material security breaches or operational outages.	Pioneering	7%
Develop and enforce control assessment standards for assessing third party use of significant fourth parties.	No Data	No Data
Conduct expansive assessments of material fourth parties in cases where the fourth party is also your third party.	Ploneering	7%
Maintain a list of service providers that are not allowed for use. These might include hosting providers that may not provide sufficient security capabilities, such as 'free web hosting' providers, or that provide 'bullet proof' hosting for potentially unethical use.	Pioneering	3%

"Our next push is to better understand and manage our concentration risk. What providers are our third parties using? Are these fourth parties protecting our assets?"

- Global Financial Institution

CAPABILITY

GEOLOCATION AWARENESS

WHAT

Know third-party system geolocations. Monitor for illegal or risky geographies, which may shift over time due to regulations, geo-political tensions or natural disasters.

WHY

Knowledge of system geolocation is essential to ensuring that you are not doing business in countries sanctioned by OFAC, or under EU Embargo or UN Embargo.

Third-party system geolocation awareness is also helpful for arming the disaster recovery and business continuity teams with intelligence to better handle geo-political risk exposure and natural disasters.

HOW

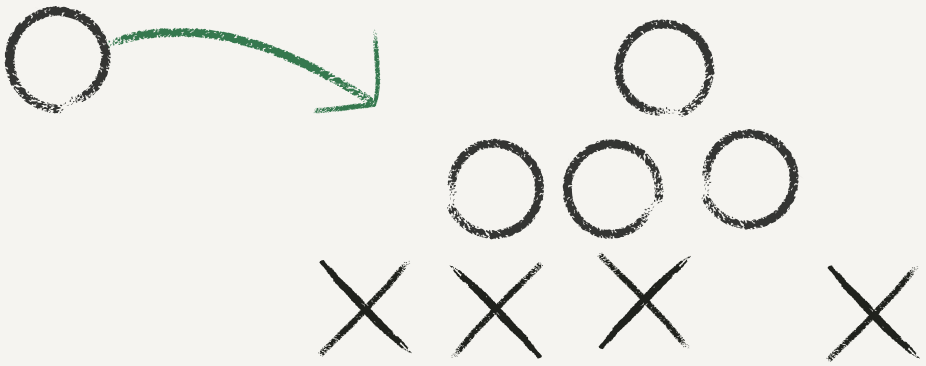
Faciliate this capability by implementing the continuous surface risk assessment capability.

Identify the geolocation of third-party systems through system IP address geolocation mapping data. Monitor system locations for regulatory compliance. Provide third-party system geolocation data to the business continuity and disaster recovery teams to aid them in managing exposure to geopolitical risks and natural disasters.

PRACTICE	STATUS	ADOPTION
Know the geolocation of third-party systems.	Pioneering	10%
Monitor significant geographies for events that may impact your operations.	Pioneering	7%
Maintain a list of geographies where system hosting is not allowed.	Pioneering	20%

"We leverage our visibility into the geolocation of third-party systems to help our disaster recovery team better manage through natural disasters. For example, when the hurricanes were bearing down on Houston, our DR team used our data to understand which partners were potentially exposed.

- Natural Gas Company



INVITATION TO PARTICIPATE

We invite you to participate in the *Playbook* study. It is literally a collection of the third-party risk management capabilities and practices deployed by enterprises of all types across the world. Join in and share your insights and expertise. As you gain from the generosity of others, others will gain from yours and as a community we can better control third-party risk.

We will publish major study updates annually and minor updates semi-annually. As such, your input will be quickly re lected in the *Playbook*.

A study sponsored by RiskRecon, Inc. | WWW.RISKRECON.COM

ABOUT US

RiskRecon, a Mastercard Company, enables you to easily achieve better risk outcomes for your enterprise and your supply chain. RiskRecon's cybersecurity ratings and assessments make it easy for you to understand and act on your risks, delivering accurate, risk prioritized action plans custom-tuned to match your risk priorities. Learn more about RiskRecon and request a demo at www.riskrecon.com.

Deep transparency. Strong accountability. Continuous collaboration.

COPYRIGHT