whistic | riskrecon mastercard

The Modernization of Cybersecurity

How Technology is Changing the Way Businesses View Vendor Assessment and Cybersecurity: A joint research project between Whistic and RiskRecon, a Mastercard company

Introduction

Third-party risk management is the process of holding organizations accountable to good security practices. Essentially, as you improve the security of third parties you improve the collective security of all digital supply chain ecosystems, while decreasing the likelihood of data being breached.

However, third-party risk management can be challenging. It requires deep transparency, strong accountability, effective collaboration, and swift action, all inputs exacerbated by outdated, manual risk monitoring practices and further intensified by today's unprecedented rise in nth party risk.

Luckily, over the last five years, there has been an evolution in the development of cybersecurity and vendor assessment tools focused not only on keeping businesses secure, but also on streamlining and simplifying the process along the way.

It is with this backdrop Whistic and RiskRecon, a Mastercard Company, set out to discover key trends in cyber risk management, vendor assessments, and understand how new technologies are creating greater efficiencies, and unpack the business implications brought on by these innovations.

Key Findings

Executive Summary

Whistic and RiskRecon, with the help of a third-party research firm, surveyed more than 500 cybersecurity and third-party risk practitioners to capture current trends impacting the industry. Respondents ranged from managers (30%), directors (28%), and executives (42%) that worked mainly in small, medium, and enterprise businesses with a small number coming from startups.

Organizations of all sizes are placing a greater focus on cybersecurity in the past 5 years

As the threat of third-party security incidents continues to loom large, most businesses are taking the threat seriously and have implemented programs to monitor and manage the cyber risk of third-party vendors.

- 80% of businesses have a cyber risk monitoring and management program in place.
- 60% of businesses have incorporated more technology to manage the process in the last five years.

Modern technology has helped accelerate the maturity of cyber risk and vendor security programs

As the use of technology has increased, it stands to reason that the maturity of cyber risk and vendor security programs have as well.

However, start-up companies are less likely to have advanced programs compared to enterprise-level companies.

- 66% of enterprise-level companies have advanced stage programs, while 8% have early stage programs.
- 6% of start-ups have advanced stage programs, while 64% have early-to-non-existent programs.

Cybersecurity is a concern at all levels of the organization, including the c-suite

Because of the impact third-party incidents have across the entire organization, both from the cost to remediate once they're discovered and the damage they cause to customer trust and brand perception, cybersecurity programs have the attention of the executive level.

However, there are subtle differences in priorities regarding program success metrics amongst levels within the organization.

- Executive leaders rank (1) Accuracy of Findings, (2) Program Cost, and (3) Remediation of Issues as their top three measures of program success.
- Yet, security risk partitioners rank (1) Accuracy of Findings. (2) Security and Legal Compliance, and (3) Vendor assessment completions as their top three measures of program success.

Trust but verify is still a staple in the industry

Most organizations still rely on and trust traditional methods of vendor risk monitoring such as questionnaires and assessments.

- 53% of respondents say that they trust the information they receive from their vendors.

However, most respondents are increasing the frequency in which they validate information and are employing third-party monitoring tools to do so.

- 61% of respondents validate vendor questionnaire responses with a third-party tool.
- 43% of respondents have started using risk scoring to evaluate vendors within the last five years.
- 40% of respondents are validating responses every six months, 30% are validating once a year, 7% every other year, and 21% it depends on the vendor.

Section 1

Current state of cybersecurity programs

The cyber-attacks that once made headlines involved vast breaches from a single company. However, today's cyber-attacks have become more complex as the number of business relationships (vendors, suppliers, partners, etc.) an organization engages with has increased; thus, amplifying their overall risk exposure.

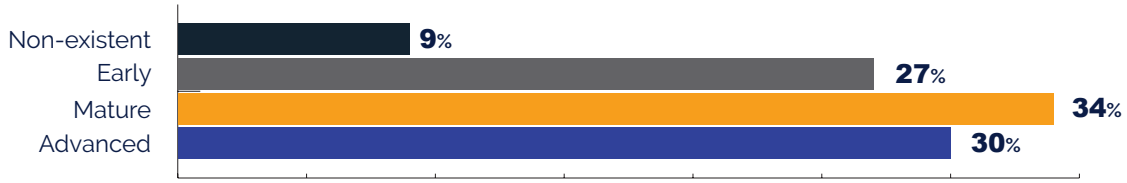
Luckily, advancements in technology are helping organizations of all sizes to quickly and more readily identify, assess, and take steps to remediate cyber risk within their digital ecosystem. Proving a cybersecurity program is no-longer a nice-to-have—but a must have for any organization.

Do a majority of businesses have cyber risk monitoring and management programs in place?

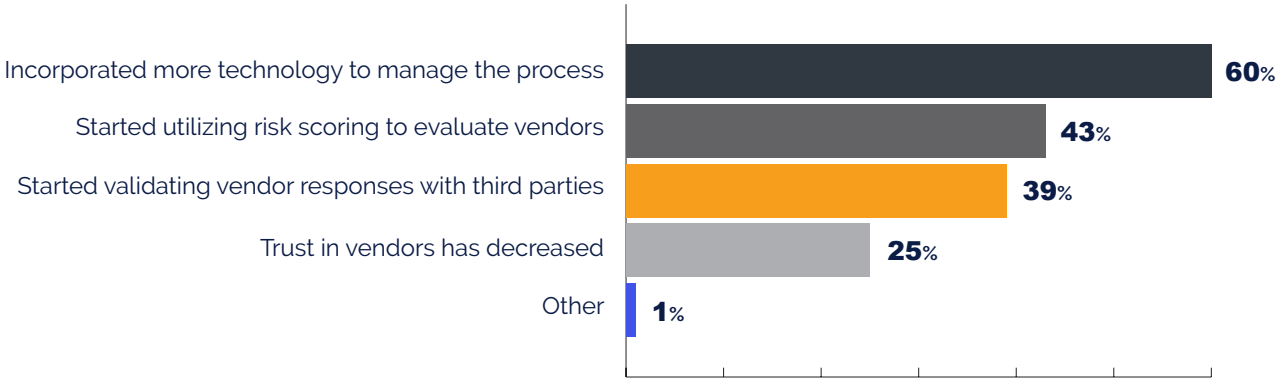
have a cyber risk monitoring program in place

do not have a cyber risk monitoring program in place

What is the maturity of most cyber risk management programs?



How have vendor security programs changed in the last five years?



Section 2

Significance of cybersecurity gaining traction at the executive level

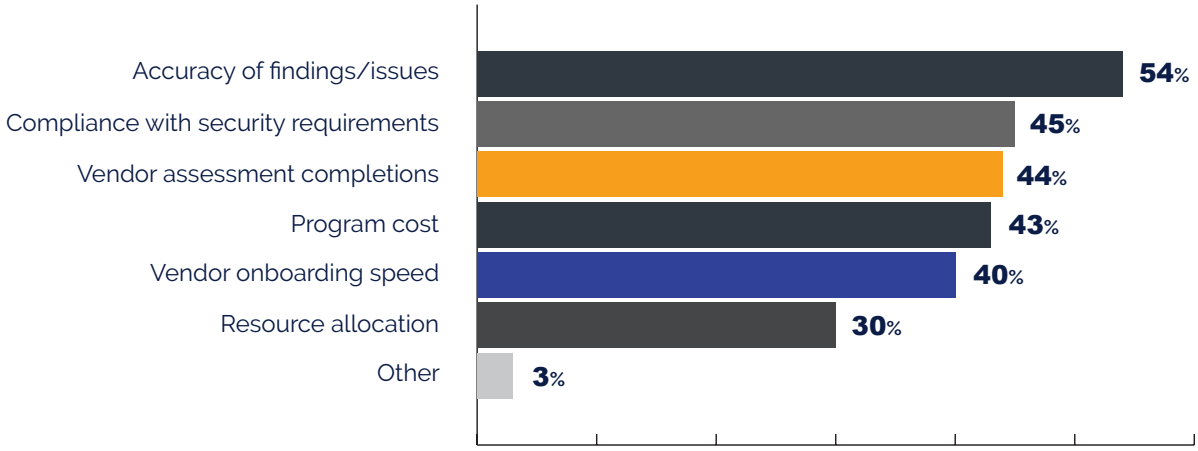
As the world has transitioned from on-premise to cloud based solutions, the protection of customer data being handled by third parties has grown in importance. Cybersecurity and third-party risk are no-longer problems that concern only IT and InfoSec teams. Because of the impact a data breach can have on the entire organization, this function has the attention of the highest levels of many companies.

Do a majority of cybersecurity programs report programs to leaders outside of the organization?

71% of respondents report program metrics to internal leadership outside the org

29% of respondents do not report program metrics to internal leadership outside the org

What are the top KPIs for measuring the success of cyber risk programs?



Which metrics are most important to executive leadership?

1. Accuracy of findings/issues
2. Program cost
3. Remediation of findings/issues
4. Vendor assessment completions
5. Resource allocation
6. Vendor onboarding speed

Section 3

Trust in vendors is increasing, but third-party validation still needed

In the era we live in, it can be difficult for companies to trust the information provided by vendors. This has been encapsulated in the zero-trust philosophy prevalent in recent years. However, trust in vendors is increasing as companies realize the best way to stay ahead of bad actors is by forming collaborative relationships with their vendors to create a more secure defense. Nonetheless, just because trust is increasing, it doesn't mean companies shouldn't perform the necessary due diligence to validate data provided to them by their vendors.

Do companies trust the questionnaire responses they receive from vendors?

- 53% Agree
- 36% Somewhat agree
- 10% Neutral
- 1% Disagree

Are companies conducting third-party validation of vendor questionnaire responses?

- 61% Yes
- 39% No

Has the use of third-party validation increased in the past year?

- Yes (41%)
- No (51%)
- Not applicable (8%)

How frequently are companies validating third-party questionnaires?

- Every six months (38%)
- Once a year (34%)
- Every other year (7%)
- Depends on the vendor (21%)

Recommendations

Based on the survey results, we've compiled some recommendations that will help businesses improve both the efficiency and speed of their programs while maintaining the accuracy of vendor assessment data while ensuring compliance in a world with increasing regulations.

Improve the efficiency and speed of your program while keeping costs at a minimum

Despite how important vendor assessments are in helping to prevent future data breaches, the investment in technology hasn't always been commensurate. Up until recently, most vendor assessment programs were managed with spreadsheets and emails. Keeping track of the security posture of all the vendors a company used was a near impossible task using those remedial tools. The end result was slow buying cycles and iffy security.

Luckily, there are a number of tools available (Whistic included) that simplify and streamline the vendor assessment process through automation. Below are some ways to incorporate technology into your program to improve the speed and efficiency of your program.

Vendor intake and automated risk scoring

The first step in the vendor assessment process can be one of the hardest if not done right. When adding a new vendor, it's critical that you gather all of the information up front. Doing so will help the InfoSec team determine the inherent risk associated with vendors before initiating a formal security review.

One of the best ways to accelerate the vendor intake process is putting the onus on the requestor to gather all the information needed via a vendor intake form. This eliminates the need for the InfoSec team to go on a wild goose chase tracking down what is needed to initiate the process. A good vendor intake tool will automatically notify the InfoSec team once the form is submitted and assign an initial risk score based on the answers provided. The risk score will evaluate a number of different criteria, including software patching, application security, web encryption and determine system risk value based on system sensitivity and data at risk.

Security ratings tools are a great way to quickly measure and assess how good or how poor the cyber hygiene of a given organization is. In fact, many cyber risk scoring tools can

legally scan an organization's cyber posture without any additional permissions or input from an organization—often rendering easy to understand A–F or 1 to 10 scoring metrics in a matter of minutes (RiskRecon included).

Automated follow-up

Once the security review is initiated, you need to ensure that vendors are responding in a timely manner. With everything an InfoSec practitioner already has on their plate, it can be difficult to stay on top of the status of each vendor assessment in the queue, especially when you consider they are assessing more than 14 vendors per month on average. However, when a company implements a vendor assessment tool to manage the process, the status of each assessment is easily monitored and when vendors have stalled on completing a questionnaire, the tool will automatically send out a reminder to nudge them to the finish line.

Conducting zero-touch assessments

Another way to accelerate the vendor assessment process is by accessing previously completed questionnaires that have either been published to a vendor's website or a directory like the CSA STAR Registry or the Whistic Trust Catalog. When done right, an on-demand security profile provides you with everything you need to conduct an assessment, including completed standard questionnaires and frameworks and other relevant security documentation without having to engage in a lengthy back and forth with the vendor just to collect the information.

Automated reassessment

Finally, to ensure you have up-to-date information about a vendor's security posture, it's important to conduct reassessments on a regular basis. Depending on the riskiness of the vendor this could be as often as every six months or as infrequent as every other year. To ensure you never miss a reassessment, it's important that whatever tool you implement allows you to set the time frame for reassessment and have the requests sent out automatically.

Ensure accuracy of your vendor assessment and risk data

Trust is a major pillar of third-party risk management. You have to trust the vendors you do business with, you have to trust their questionnaire responses, and you also have to trust the technology tools you use to validate them. Hence why accuracy of findings is so vital.

Having confidence in data and insights makes all the difference when you are faced with having to make too many risk decisions. Validation tools that only provide a laundry list of findings, plagued by false-positives create a panicked battleground of misinformation. When organizations can't quickly decipher between a real threat or a non-threat, either because their validation tool does not prioritize the findings by potential impact if infiltrated or because the findings themselves are inaccurate, data loss events are more likely to occur.

Security ratings tools with high rates of accuracy, like RiskRecon—independently verified at 99.1% accuracy—allow you to create custom risk alerts based on your organization's priorities, helping your firm to achieve better risk outcomes. RiskRecon's Issue Risk Matrix provides organizations with instant visibility into the risk distribution of security issues across their entire vendor portfolio enabling them to identify vendors that have issues within their risk priority settings.

Maintaining compliance in a world with increasing regulations

In recent years as companies gained access to more and more private, customer data, governments in many geographies developed regulations geared towards protecting their citizens from having that data exploited or compromised due to lax security standards. Although laws like GDPR in the EU and CCPA in California were created to protect citizens in those areas, they apply to all entities that collect and process data from residents in those areas.

As noted earlier, maintaining compliance with these types of regulations is one of the top KPIs for InfoSec practitioners surveyed for this report. To ensure compliance has been achieved, we recommend self-assessing against the questionnaires and frameworks associated with the laws and regulations your business is subject to.

Once each questionnaire is completed, it's easy for you to identify security controls you need to improve upon in order to become compliant. This process can be easily managed using a tool like Whistic Profile that has many of the questionnaires needed like the aforementioned GDPR and CCPA along with others like HIPAA. The tools enable your entire team to collaborate on the self assessment, identify potential problem areas, and build out a plan of action that ensures any shortcomings are addressed.

Conclusion

In the past five years, the entire IT application and outsourcing landscape has shifted for most companies. Previously, most companies relied on a relatively small number of IT providers and resellers and most software and data ran from the company's own data center.

As the delivery of software and services over the public internet (SaaS) became far more efficient and innovative, many organizations began shifting from an on-premises software model, where companies would visit the third-party vendor's data center to validate risk processes, to a more technology-driven approach.

However, over time the number of vendors used at a particular organization has continued to increase, while the size and sophistication of security teams decreased. Thus, their ability to consistently design and maintain good security and data protection practices became more limited.

Yet, with all the growing risk and complexity described above, most vendors return their security questionnaires looking very good. Often too good for an experienced risk or security person to believe. They are not frequently lying, but rather describing their documented procedures which can vary considerably from the reality of what they are doing in practice. And, even if the processes were working, the number of vendors and risk has grown too large to be managed with a manual process of people and spreadsheets.

The current vendor questionnaire process can't be replaced completely as there are some items that can only be known by asking the vendor themselves—e.g., their disaster recovery plan, their employee background check procedures, etc. Vendor assessment and risk validation technology tools like Whistic coupled RiskRecon can bring a scalable way to obtain objective and actionable security performance information for your own organization and your third parties.


whistic
riskrecon
mastercard