WHITEPAPER

How to measure, manage, and mitigate third party risk in real-time

January 2022

SAFE

INTRODUCTION

It is common place for third parties to have access to an organization's data and systems to provide software and services integral to operations across the enterprise. The average organization uses nearly 6000 third party SaaS applications[1] to simplify business functions ranging from prospect and client management to handling accounts. Leveraging SaaS solutions results in gained time, economic efficiencies, and essentially enables the organization to remain competitive in the market. However, these solutions, and therefore the vendors themselves, often have unsupervised access to critical data. The Ponemon Institute reports[2] that while many businesses continue to outsource critical business processes to third parties, 63% of organizations don't have visibility into the level of access and permissions for both internal and external users, and have a limited-to-no view of:

- the extent of third party access to their network,
- when third parties access their network,
- why third parties have accessed their network.

In recent years we have seen vulnerabilities in third party software in particular hit the mainstream media - spreading far beyond the IT and business communities. These vulnerabilities rank in the top 5 of the most expensive data breach vectors with an average cost of $4.33 million per attack[3]. Dubbed 'the biggest ransomware attack on record', software provider Kaseya hit the headlines in 2021[4] when it was attacked by the REvil Ransomware-as-a-service group. Hackers breached their remote monitoring and management technology giving them access to clients of several Managed Service Providers that used Kaseya's services for their business. REvil demanded $70m in ransom.

Without the correct technical and contractual controls, inadequate Third Party Risk Management (TPRM) is equivalent to inviting a data breach home.

The importance of fourth and *nth* party risk in cybersecurity assessments

An organization inherits most of its cyber risks from its direct and extended vendor network. Businesses have shifted from regular and planned touchpoints with contractors to making several cybersecurity exceptions to facilitate seamless remote work. This, while aiding speed and efficiency, reduces cybersecurity to an afterthought due to reduced insights, thereby increasing the likelihood of a breach.

While an organization may have a strong risk management strategy to manage third party risks, **risks arising from fourth party vendors are not always monitored.** In short, they are your third parties' vendors and this should be an important consideration within any cybersecurity risk assessment. Without a clear understanding of the business relationships and attack surface of the extended ecosystem, any sort of data compromise could threaten the organization, creating liability.

Third parties themselves must build a robust risk management strategy of their own to ensure fourth parties are adequately assessed. While SOC 1 and 2 certification and Statement on Standards for Attestation Engagements 18 (SSAE 18) have made fourth party cyber risk identification easier, it is often a manual process that is often overlooked.

The Global Third Party Risk Management Survey 2021[5] states that more than 50% of organizations want to improve real-time information, risk metrics, and reporting in the year ahead so they have a single, up-to-date picture of their *nth* parties and the risk they may pose.

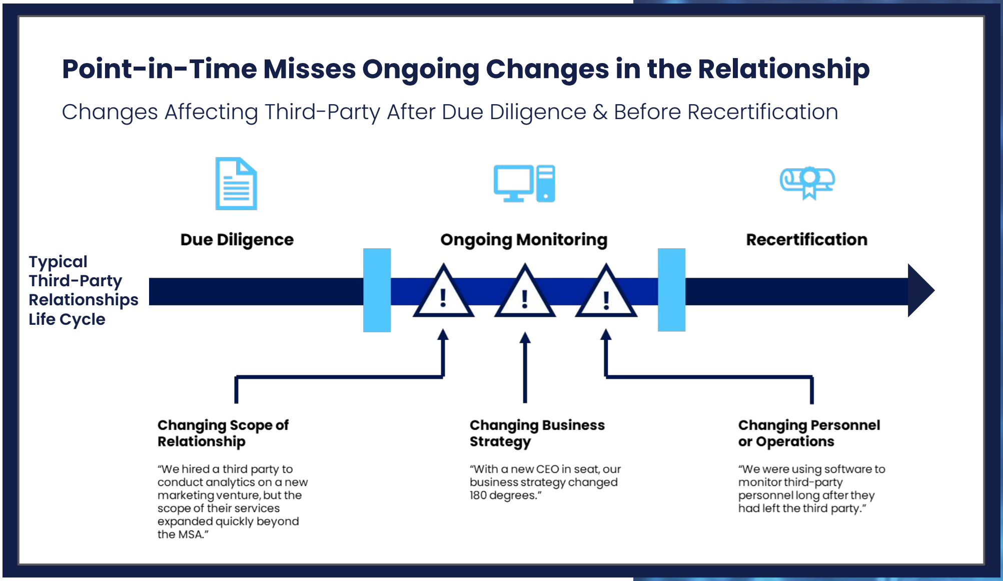
To achieve this, organizations need to change their approach by moving beyond static, point-in-time risk and vulnerability assessments. **They should adopt a strategy of automated, dynamic risk quantification**, with an inside-out and outside-in assessment of their digital footprint across endpoints, cloud assets, and SaaS applications - which extends to third parties and their vendors. Until organizations begin to continuously measure and quantify their level of risk in real-time, their ability to prevent a breach from taking place is heavily restricted.

The limitations of modern vendor risk management

According to Gartner[6], more than 80% of legal and compliance leaders tell us that third party risks were identified after initial onboarding and due diligence, suggesting **traditional due diligence methods in risk management policy fail to capture new and evolving risks.**

Gartner states that the ideal flow of third (*nth*) party assessment should begin with a formal evaluation and written report, however, it needs to be supplemented with Security Rating Services ensuring 360-degree coverage. *Going beyond basic vendor policy assessments via questionnaires and outside-in Security Rating Services, businesses need a real-time assessment of their third party's critical systems via an inside-out approach.*

Today, 51%[2] of organizations are not assessing all of their third parties before granting access to their networks[7]. This poses the question: Do the remaining 49% of organizations have visibility of the true third party network and data's real-time cyber risk posture of their network?



Point-in-Time Misses Ongoing Changes in the Relationship

Changes Affecting Third-Party After Due Diligence & Before Recertification

Typical Third-Party Relationships Life Cycle

Due Diligence

Ongoing Monitoring

Recertification

Changing Scope of Relationship

"We hired a third party to conduct analytics on a new marketing venture, but the scope of their services expanded quickly beyond the MSA."

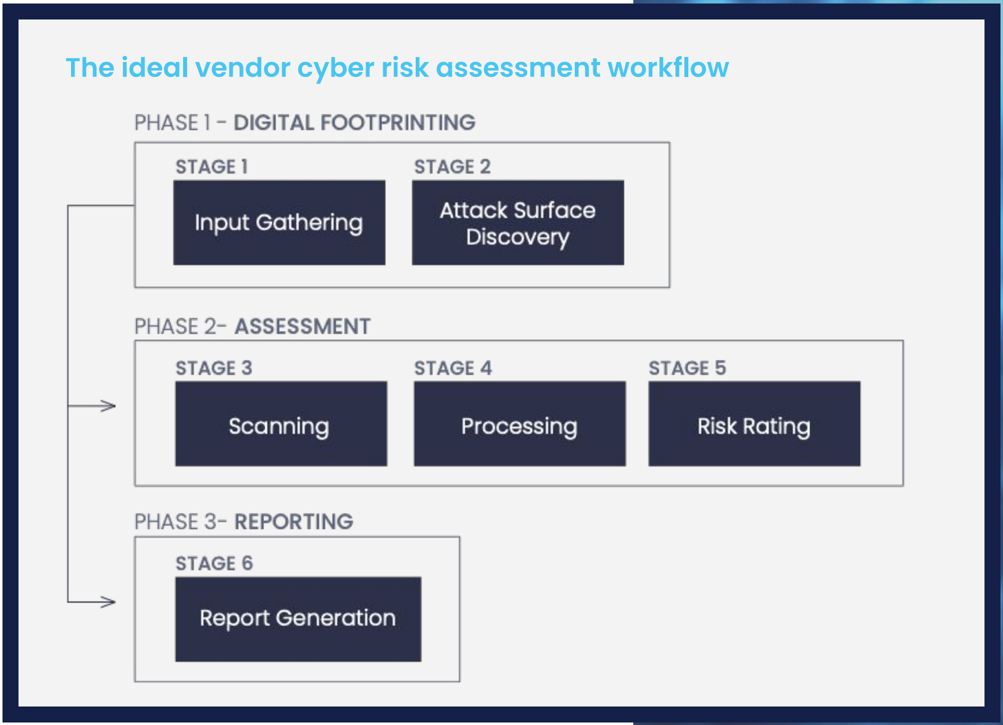
Changing Business Strategy

"With a new CEO in seat, our business strategy changed 180 degrees."

Changing Personnel or Operations

"We were using software to monitor third-party personnel long after they had left the third party."

Figure 1 : Point-in-Time Misses Ongoing Changes in the Relationship, Gartner[6]



The ideal vendor cyber risk assessment workflow

PHASE 1 - **DIGITAL FOOTPRINTING**

STAGE 1: Input Gathering

STAGE 2: Attack Surface Discovery

PHASE 2- **ASSESSMENT**

STAGE 3: Scanning

STAGE 4: Processing

STAGE 5: Risk Rating

PHASE 3- **REPORTING**

STAGE 6: Report Generation

Figure 2: Vendor risk assessment workflow, Safe Security[7]

How to quantify third party cybersecurity risk

A vital component of Cyber Risk Quantification is the mathematical scoring model used to calculate and report risk. Within this field, there are several models available - the most popular being the Bayesian Network model - which will be the method we focus on in the remainder of this whitepaper.

- **Bayesian Network**
- Weighted average
- Log odds
- MaRiQ[8] (Manage Risks Quantitatively)
- Logistic regression
- Multilayer neural networks

What is the Bayesian network?

The Bayesian Network is defined as a method for 'taking an event that has occurred and predicting the likelihood that one of the several possible known causes was a contributing factor'[9]. When applied to Cyber Risk Quantification, it calculates the likelihood of organization being breached within 12 months.

Method

The initial level of information (or, initial breach probability) is updated with new information received from the continuous third party risk assessment.

The initial probability is used as the first level of input in the metadata, where the probabilities corresponding to geography, size, industry, and exposure of a customer are combined to derive the breach probability solely based on the profile of a customer.

This breach likelihood calculation, based on the profile of the customer, is applied to all the security domains. As per the underlying controls state (ie. Qualified and/or Failed), the likelihood of breach for each security domain is estimated.

Each security domain produces a breach probability score. The output from each of these domains is combined, which gives the final breach probability for the estimation of the third party risk score.

Profile information

- The organization's geography
- Industry type
- Size based on revenue
- Number of exposed assets

Security Domains and Weightage

Security Domains	Security Domain weight
Email Security	Low
Application Security	Medium
Network Security	High
Breach Exposure	Medium

Security Domains	Security Domain weight
System Security	High
Compromised Systems	Low
Cyber Reputation	Low
DNS Security	Low

Checklist: Find a solution that will effectively quantify third party risk

Not all Third Party Risk Management solutions are equal. To help you navigate the market and find the best solution for your organization, use this checklist for your research.

360-degree assessment	❏ Does the vendor risk assessment begin with a questionnaire? ❏ Does it determine what information is critical for your company based on your geography, industry, and revenue? ❏ Does it provide outside-in Security Rating Services? ❏ Does it cover all of your digital domains? Such as email, network, applications, etc. ❏ Does it integrate with your existing security tooling via API? ❏ Does it provide an assessment of your cloud providers/estate? ❏ Does it perform an assessment of your vendors' employees? ❏ Does it map your vendors to your unique regulatory and compliance standards and requirements?
Continuous assessment	❏ Does it measure your *nth* party cyber risk in real-time? ❏ Does it produce an accurate, real-time risk score? ❏ How often does it conduct assessments? Daily, weekly, monthly scans, or a combination? ❏ Is it able to monitor your vendor and detect changes within the third party relationship? ❏ Does it categorize your vendors into tiers to determine the frequency of assessment?
Credibility	❏ Does the solution corroborate multiple data sources to understand current and potential data breaches? ❏ Does it correlate the data with past reports, audits, and settlements? ❏ What is its false-positive record? ❏ How often are the standards and controls within the service or solution updated and implemented?

Contextual reporting	❑ Does the solution report the likelihood of third party data breaches? ❑ Does it present all your risks on a single dashboard? ❑ Does it report the potential financial impact of a data breach on your business? ❑ Does it provide macro and micro scores for the security team? ❑ Does it benchmark your risk posture against others in your industry?
Mitigating risk	❑ Does the solution deliver actionable mitigation strategies or countermeasures for the risks it detects? ❑ Does it embed controls and incentives to manage high-risk third parties and improve ongoing monitoring? ❑ Are the countermeasures and insights prioritized according to your business requirements and threat profile?

CONCLUSION

Third parties will remain an integral part of an organization's business operations. As dependency on these vendors increases to remain competitive, the level of risk to their assets and data will also increase. This needs to be reflected in every organization's cybersecurity strategy and planning to avoid crippling attacks such as those on Kaseya, SolarWinds, Trinity, Marriott, and more.

A strategy that purely focuses on and assesses direct third party vendors is no longer sufficient. Organizations require visibility of their nth party ecosystem - monitoring each of their SaaS applications, individual risk postures, and independent policies — with the same diligence they exercise when monitoring subsets within their own business. The best practice is to take data-driven control of nth party cyber risks via granular monitoring and real-time auditing of third party access using machine learning-enabled cyber risk quantification solutions.

By using your understanding along with the checklist within this whitepaper, you will be well on your way to finding the most effective and efficient cyber risk quantification solution for your business. It will ensure that your organization is doing all it can to measure, manage, and mitigate third party risk.

References

1. Digital Transformation and Cyber Risk: What You Need To Know To Stay Safe [Internet]. 2020. Available from: https://get.cybergrx.com/ponemon-report-digital-transformation-2020
2. A Crisis in Third-Party Remote Access Security | SecureLink [Internet]. SecureLink. 2021. Available from: https://www.securelink.com/research-reports/a-crisis-in-third-party-remote-access-security
3. Cost of a Data Breach Report 2021 [Internet]. ibm.com. 2021. Available from: https://www.ibm.com/security/data-breach
4. Who’s behind the Kaseya ransomware attack – and why is it so dangerous? [Internet]. The Guardian. 2022. Available from: https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers
5. Global Third Party Risk Management Survey 2021 [Internet]. Deloitte Switzerland. 2021. Available from: https://www2.deloitte.com/ch/en/pages/risk/articles/third-party-risk-management-global-survey.html
6. Third Party Risk Management and Mitigation | [Internet]. Gartner. 2021. Available from: https://www.gartner.com/en/legal-compliance/insights/third-party-risk-management
7. Vendor risk assessment workflow, Safe Security
8. Carlsson E, Mattsson M. The MaRiQ Model: A quantitative approach to risk management in cybersecurity [Internet]. Diva-portal.org. 2019. Available from: https://www.diva-portal.org/smash/get/diva2:1323684/FULLTEXT01.pdf
9. Bayesian network - Wikipedia [Internet]. En.wikipedia.org. Available from: https://en.wikipedia.org/wiki/Bayesian_network

About Safe Security

Safe Security takes the guesswork out of cybersecurity. As global leaders in Cyber Risk Quantification (CRQ), Safe is on a mission to become the de-facto industry standard to measure, manage, and mitigate cybersecurity risk. We enable organizations to quantify enterprise-wide cyber risk in real-time across people, process, technology, and third parties - extended to *nth* party.

We assimilate cybersecurity signals, external threat intelligence, and business context, and distill the information to generate a single risk score. Organizations can dynamically predict the likelihood of a breach and understand the financial impact of a data breach. In addition, Safe Security gives prioritized, actionable insights that are tailor-made for your enterprise to help you improve your cybersecurity posture on a continuous basis.

Backed by ex-Cisco CEO, John Chambers, and senior executives from Softbank, Sequoia, PayPal, SAP, and McKinsey & Co., Safe Security regularly contributes to government and community-driven projects, such as the US Government's National Vulnerability Database, and the ATT&CK MITRE framework.

The SAFE Scoring Model

The SAFE scoring model is a joint research collaboration between Safe Security and MIT, Boston that incorporates cybersecurity sensors' data, external threat intelligence, and business context. It aggregates this data within a supervised, Bayesian, risk quantification engine utilizing machine-learning technology. This produces a real-time breach-likelihood score and the financial impact of potential data breaches.

For the first time, cybersecurity risk can be communicated as a single score - the one score that matters - giving organizations the confidence to predict cyber attacks before they happen.

SAFE

www.safe.security | info@safe.security

3000, El Camino Real,
Building 4, Suite 200,
Palo Alto, CA - 94306