ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Third Party Risks and their Impact to the Overall Risk Posture, how to Improve it?

Pranith Shetty

Information Security and Risk Lead, Cisco, New Jersey, US

ABSTRACT

This article is aimed at giving insight onto the various trends resulting into third party risks, categories of the risk that follows, and its overall impact to the Risk posture. It also aims at providing context on the various risks and describes a method or process that can be leveraged to mitigate those aforementioned risks. Third parties are the need of the hour in this competitive world of business, where some firms are struggling to break even. In such scenarios, employing third party resources save a lot of time, effort and capital in achieving objectives aimed at the business vision, gives you that competitive edge not just to survive but thrive. Third party risks have been existent since inception of this concept, firms should not fear employing third parties for the very same reason, there are mere hiccups, instead they should look at solving those problems with some of the approaches listed in this article.

***Corresponding author**

Pranith Shetty, Information Security and Risk Lead, Cisco, New Jersey, US.

Received: November 02, 2022; **Accepted:** November 10, 2022, **Published:** November 19, 2022

Keywords: Information Security, Cybersecurity, Information Security Managers, Financial Services, Risk Management

Introduction

Third party is a beneficial and widespread concept for quite some time now in the industry across different sectors like finance, manufacturing, technology. Businesses have been working with other firms to be successful, save time and resources since time immemorial [1]. 3rd (Third) parties offer a competitive edge since certain firms are hired as third parties because of their expertise to handle certain problems or come up with innovative solutions.

Third party risk is any risk associated with engaging a third party in context of providing a service or product to a client [2]. It is an all-encompassing term that intends to cover all risk types derived out of the relationship between firms.

Rationale for Study

More often than not, firms hiring third parties perform their due diligence, look over their financial and cybersecurity related issues etc. There are overarching contractual terms signed and executed, however, due to varied reasons, firms might run into issues with their third parties due to noncompliance on certain controls, or their failure to patch some critical, time sensitive vulnerabilities. There could be a recent data breach that the vendor or third party has been impacted with data breach or cybersecurity related attack like SolarWinds. Also in some cases third party related risks don't get the deserved attention and scrutiny within the firm, these risks are blindly accepted without a proper review by the Information security and related Subject Matter experts (SMEs) including management personnel.

Risks resulting from all of these exposures impact the overall risk posture of the overarching entity or hiring firm so it's very important to have a framework or a program that ensures these risks are brought into the fold, reviewed at least annually. They should also be brought to the attention of senior leadership and management to ensure contractual obligations are taken care of at the highest possible seniority level. Thus ensuring that there is a framework or process to deal with these risks not only proactively, ahead of time but as part of Business as usual (BAU) operations and reactively, if need be.

Trends

There are a few emerging trends that drive Third party risks [1].

• **Vulnerability Management and Incident Management Related Risks and Issues:**

Suppliers and vendors are not proactive in terms of handling vulnerabilities in their systems, they shy away from timely pacth management of their system, this results in them being open to ransomware and other threats similar to Zero day attacks.

Absence of robust incident management program on the other hand delays identification of incidents that might result in delayed communicating to the overarching firms that are impacted, all of this results in both third parties and the hiring firms open to Incidents

• **Increased Scrutiny from Regulators**

Since most of the third parties are smaller in scale, they try to mask their operating environment from some of the mandatory regulations, regulators now are increasingly focused on these third parties and also because of the cascading impact to the hiring firm which might be a critical national infrastructure holding customer data etc.

• **Financial Capacity of the Third Parties**

Financial reports of third parties are crucial in many cases, since a bankrupt or closer to bankruptcy condition of a third party would leave the hiring firm prone to significant threats. This does not give enough time for the firms to hire new vendors

Common Risks

Working with third parties enables organizations and does create a competitive edge but it does pave the way for some inherent risks [3]. In the world of Risk management as defined by NIST here there are many types of risks. These risks need to be mitigated in order to have a sustainable and long term future [4].

As we can see in the below visual, these are some of the types of risks that firms working with 3rd parties come across, there are severe implications but at the same time ensuring the following items; if put in place can help avoid these risks and ensure coverage in case of impact from third party risks.

Appropriate vendor due diligence, ensuring the basic checks, BC/DR (Business Continuity and Disaster recovery) plans, back up plans, 3rd party attestations making sure independent reviews are performed and TPRM (Third party risk management) program meant to identify, respond and report on those risks.

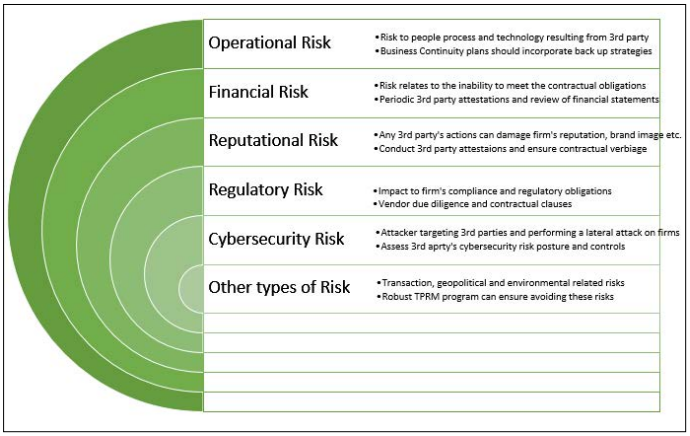


Figure 1: Common Risks Associated with 3rd Party Relationships

Literature Review

As per this article by the consulting firm " Risk Optics" there is an inherent need for programs like VRM (Vendor risk management) and TPRM (Third party risk management), some firms have had it for a short time while some firms are starting to build them now [5].

This article lists the important of Vendor risk assessments to identify and proactively mitigate risks [6].

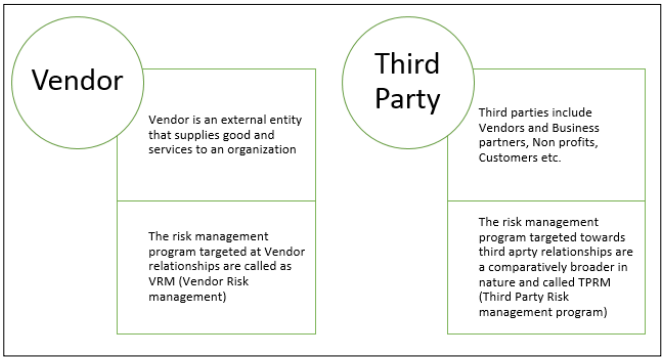
As per the consulting firm GEP in this article, they list how we can structure a VRM program in detail and what are the benefits of the program [4].

OneTrust a leading product and consulting firm in the risk and privacy space, explains here the VRM program and the importance of this program from their product perspective.

Method

Vendor vs Third Party

When we think about Third party risks, both terminologies; Vendors and Third parties are used interchangeably and sometimes mixed up conceptually, hence it's important to clarify the definitions and slight variances in both risk management program.



The most important thing in case of Third party relationships is to have an efficient and transparent TPRM; also known as third party RM program, an organization needs to have dedicated, skilled staff and resources to onboard third parties including vendors.

TPRM staff need to work with finance and contracting personnel on streamlining onboarding procedures, there should be proper due diligence performed prior to onboarding.

A Few Checklist Items to Keep in Mind are

1) Financial statements, to make sure the 3rd parties are able to support the organization both short term and long term
2) Cybersecurity related exposures, similar to SolarWinds attack where attackers gained lateral movement to organization having SolarWinds as 3rd party, its important to understand their cybersecurity risk posture
3) 3rd party attestations, its important for the organization to ensure that they provide independent attestation reports meaning performed by a different agency and not internal, These reports should attest to the operating control environment and be compared against some of industry leading certifications and frameworks
4) There needs to be contractual verbiage that holds 3rd parties accountable for their actions with respect to risks and fines to be levied statement so that organization can transfer some of the risk in case of an attack caused by them

The TPRM program staff and lead should report into the head of the governance and risk programs in the firm, this ensures all the risks identified have the necessary oversight, and the Risk reporting mechanism employed by Risk management teams would ensure Senior leadership visibility.

An alternative approach that seems to work is the TPRM function should attend the governance forums held by Risk teams and they should be presenting Critical/High and other risks on a predefined cadence, this process ensures the risks are reviewed for appropriate risk response from management. Risks below the Risk appetite and/or tolerance can be accepted temporarily while the ones above have to be mitigated. The VRM or TPRM program if in place should be re-reviewed at least annually against a maturity model thus making sure there are no lapses in the program itself.

Security Scorecard is another metric that some firms employ where a holistic score is assigned to a vendor or Third party based on a varied list of factors that rely on assessments against these vendors and the scorecard is to be reviewed frequently [7]. There are certain thresholds that need to be adhered to, meaning the score of a certain vendor or third party should not fall below the threshold. If it does then the vendor needs to be reviewed and replaced in case of no improvements. This ensures that the risks

resulting form certain 3rd parties are avoided.

Discussion and Extended Use Cases

The TPRM can be implemented across businesses, there is no dependency on the organization to fall in a certain sector, the staff needs to have the required skillsets and experience to deal with an organization 3rd party relationships. Matters should be reviewed and escalated on a predefined cadence. The program when implemented properly helps organizations steer away from inherent risks resulting from the vendors thus improving their overall risk posture. This program holds the test of time in financial services sector due to increased scrutiny and stringent requirements placed by the regulators. The technology firms too have a central program to manage vendors, which are sometimes called as Vendor management programs, as a result those firms lack an exclusive Vendor risk management program

Conclusion

In spite of the risks that third party relationships bring, Organizations should not fear and shy away from onboarding vendors and similar firms. Third party relationships provide a considerable edge in terms of competitiveness to firms. There are risks that tag along with these relationships, however, those risks can be proactively, during the engagement and reactively after risk realization can be dealt with an efficient TPRM program. Risk management and governance in any firm can ensure risks including third party are navigated through the risk management lifecycle [8-10].

References

1. Tim Scott, Nathan Spitse. Third-party risk is becoming a first priority challenge. Deloitte Canada https://www2.deloitte.com/ca/en/pages/risk/articles/reduce-your-third-party-risk.html.
2. Third Party Risk. Open Risk Manual https://www.openriskmanual.org/wiki/Third_Party_Risk.
3. NIST (2022) Risk – Glossary. CSRC https://csrc.nist.gov/glossary/term/risk.
4. One Trust (2021) What is Vendor Risk Management?. OneTrust https://www.onetrust.com/blog/vendor-risk-management/.
5. Risk Optics (2022) What is Vendor Risk Management (VRM)? The Definitive Guide. https://reciprocity.com/what-is-vendor-risk-management/.
6. Kezia Farnham (2021) Vendor risk management: Understanding and mitigating third-party vulnerabilities. Diligent.com https://www.diligent.com/resources/blog/vendor-risk-management.
7. 5 Steps to Selecting a Vendor Risk Management Framework. Security Scorecard. https://securityscorecard.com/blog/5-steps-to-selecting-a-vendor-risk-management-framework/.
8. Victor Dey (2022) Third-party risk: What it is and how CISOs can address it. VentureBeat https://venturebeat.com/security/third-party-risk-what-it-is-and-how-cisos-can-address-it/.
9. Robert Teachout (2016) Conflict of Interest Is Top Third-Party Risk Management Concern. www.shrm.org https://www.shrm.org/topics-tools/news/conflict-interest-top-third-party-risk-management-concern.
10. Supplier Management Technology (2022) Vendor Risk Management: A Comprehensive Guide. GEP Blogs https://www.gep.com/blog/technology/vendor-risk-management-guide.