INFO~TECH
RESEARCH GROUP

Looking at Risk in a New Light:

The 6 Pillars of Vendor Risk Management

Winter 2023

Vendor Risk Impact Assessment Series Overview

Introduction

While discussing an old incident with a client and how it related to unexpected costs, it occurred to me that many, if not most, people do not look at the impacts of risk in the same light that I do. My experience in security, risk, and IT operations lends heavily to tracking the potential impacts of different potential risks throughout an organization's structure. Reflecting on how much the world and industry have changed over the last several years led me to write a research series highlighting different aspects of risk impacts on organizations that culminates in a final piece bringing them all together into a consolidated format.

The series encourages cross-discipline participation in a series of tabletop "what if" exercises to bring together various leadership and subject matter experts in an effort to help inform all parties on the multiple ways vendors could cause harm to their organization (either intentionally or not), as well as to work together to determine the best possible mitigations to either avoid or lessen the impacts from those incidents. To help further these exercises, I have developed and included tools that aid in quantifying various impacts of potential risks, including examples meant to be a starting point for the discussions.

Unlike many tools on the market, these focus on the impacts – rather than having the likelihood – of an incident minimizing the expected damages. Today, organizations can and should assume that they eventually will have an incident and plan accordingly. As a result, the old formula (Risk = Likelihood * Impact) no longer feels valid. Instead, organizations need to look at the risk impacts of vendor actions more than the likelihood of an incident and calculate their risk appetite and tolerance levels accordingly.

What the series does not focus on, because frankly, there is already a plethora of research on the topic, are the aspects of creating risk governance, determining overall risk tolerance and risk appetite levels, or inherent risk for organizations. The series assumes that the audience already has a basic understanding of these principles, instead focusing on potential risk impacts from vendors in different ways. More importantly, it seeks to educate the readers on the types of risk that vendors may pose to their organizations and the myriad trickle-down impacts that the organization's leadership may not fully understand.

The Six Pillars

When I started creating the risk series, the first step was creating a baseline taxonomy of the different aspects on which to focus the discussion. Considering that the central insight was that the likelihood of an event occurring in the modern era was edging closer to 100%, that meant focusing on where organizations would feel the most pain from various impacts. Targeting IT leadership as the audience, I decided on an educative, practical approach to the classification to highlight attention on the following, where the impact is a result of losses due to negative vendor actions.

Financial Risk Impacts

Example: Hospitals often rely on vendors to manage their data center environments but rarely understand the downstream financial impacts if that vendor fails to perform. For example, a vendor implements an "out of cycle" patch without notice. Suddenly, all IT systems are down. It takes 12 hours for the IT team to return systems to normal. The downstream impacts are substantial:

- No revenue was captured during the outage (patient registration, payments).
- The significant financial loss impacts cash on hand and jeopardizes future projects.
- Clinicians cannot access the electronic health record (EHR) and shift to downtime paper processes, causing potential risks to patient health, such as unknown drug interactions, and potentially incurring lawsuits, fines, and penalties.

- After correcting the incident, staff must manually add the paper records into the EHR, losing time creating paper records, and overtime is required to reintroduce those records into EMR.
- IT staff time and overtime pay on troubleshooting and solving issues take away from normal operations and could cause delays, impacting other projects' timing.

Strategic Risk Impacts

Example: In 2019, the airline industry yielded record profits of $35.5 billion. However, in 2020 the pandemic devastated the industry, with losses of around $371 billion. The industry leaders engaged experts to study how the pandemic impacted them and propose measures to ensure the survival of their industry in the future after the pandemic. They determined that "[p]recise decision-making based on data analytics is essential and crucial for an effective COVID-19 airline recovery plan" and adapted their strategic plans moving forward to encompass these results.

The recent meltdowns in 2021 & 2022 resulting from Southwest Airlines' refusal to adapt and spend the necessary resources is an example of the impact of not adjusting strategy.

Reputational Risk Impacts

Example: Someone breached the point of service (POS) systems and stole the customer credit card data from a popular local restaurant. The restaurant did the right thing: privately notified the affected people, helped them set up credit monitoring services, and replaced their compromised POS system. Unfortunately, the local newspaper got wind of the breach. It published the story, leaving out that the restaurant had already notified any affected customers and had replaced their POS machines. In response, the restaurant launched a campaign in the local paper and on social media to repair its reputation in the community and reassure people that they could safely transact at their place of business. For at least a month, the restaurant experienced drastic decreases in revenue as customers either refused to come in to eat or paid only in cash –on top of the added advertising spent outside their budget.

Security Risk Impacts

Example: Many organizations' supply chains affected by the SolarWinds incident in December 2020 are still identifying and trying to manage the impacts.

Operational Risk Impacts

Example: Awareness of the supply chain's complications and of each organization's dependencies are increasing for everyone. However, most

organizations still do not understand the chain of n-party vendors that support their specific vendors or how interruptions in their supply chains could affect them. The 2022 Toyota shutdown due to Kojima is a perfect example of how one essential part vendor could shut down your operations.

Regulatory Risk Impacts

Example: It is well established that prominent IT vendors often seek out and acquire smaller vendors to expand their portfolios or eliminate competition in the market. Many of these large vendors employ dubious practices and lack good ESG (Environmental, Social Governance) policies and procedures, while regulatory bodies in several countries are expanding their audit and enforcement practices. If an acquisition happens, organizations can find themselves in immediate peril of non-compliance with ESG regulations and face significant penalties.

The "What If?" Game

An essential part of managing risk in your organization is understanding the potential risks, where they may occur, and how they might impact your organization. We have discussed the types of risk above and how to assess risk generally, but let's now take that assessment to the individual level.

Various people in your organization will look at potential risks and their impacts differently. For just a few examples, the business process owner's perspective will focus on operational needs, the CISO will look at the security safeguards, Legal will look at contractual options, and leadership will want to know how risks will impact their strategies.

All these individuals bring multiple perspectives to the table to inform and educate all participants, creating a more comprehensive view of the situations being considered. To that end, ensure that the right people are at the table for the exercise and that only the people who need to be there are present to facilitate a more efficient tabletop exercise. The result should be a portfolio of the different potential risks, along with their impacts on the organization, and hopefully, some proposed controls to monitor and manage those risks long term.

Identify, Monitor, and Manage

A direct result of engaging in the "what if?" exercise is the identification of risks to your organization and their potential impacts should the unfortunate occur. Use the identified risks to educate the organization and enact proper mitigating steps. Never forget that identifying risk is just the first step.

In order to adequately protect the organization, they need to establish proactive monitoring and ongoing management practices to mitigate each identified risk. Ideally, proposed efforts were discussed and documented during the tabletop exercise. Still, if not, the portfolio of risks derived from that game can pass to individuals specializing in transferring and mitigating the various risk types.

Establish a reasonable cadence on each issue as well. An example would be to capture a fresh risk assessment well before any notification period on upcoming renewals. You may also look at quarterly business relationship meetings as an opportunity to revisit the performance metrics of a vendor or take stock of their current financial situation. The important thing is to make sure someone is managing the process and documenting any known or potential issues that could impact your organization well before an incident occurs.

Incorporating Lessons Learned

When issues arise, as they most surely will, good documentation and a root cause analysis will prove invaluable. The lessons learned during actual incidents are an essential source of proactive management practices. Make sure to use past negative actions and organizational experiences to strengthen your protection against future cases.

Summation

Organizations and their leaders need to understand that incidents are more likely to happen in the current world than at any prior time. Situations in the global market make the likelihood of a negative vendor interaction almost a certainty. The impacts of incidents are currently poorly understood and need a combined experiential effort to illuminate them.

Internal resources can work collaboratively to gain insight into the potential negative consequences of future incidents. The individuals involved can use past lessons learned and their own distinct operational understanding to bring clarity to the situations unfolding and educate one another on organizational processes and risks. Doing so can create a very clear picture for leaders so that they can make realistic, informed decisions on how to mitigate the impacts of those risks and better protect their organizations.

References

- Identify and Manage Financial Risk Impacts on Your Organization | Info-Tech Research Group (infotech.com)
- Identify and Manage Strategic Risk Impacts on Your Organization | Info-Tech Research Group (infotech.com)
- Identify and Manage Reputational Risk Impacts on Your Organization | Info-Tech Research Group (infotech.com)

Coming soon:

- Identify and Manage Security Risk Impacts on Your Organization | Info-Tech Research Group
- Identify and Manage Operational Risk Impacts on Your Organization | Info-Tech Research Group
- Identify and Manage Regulatory Risk Impacts on Your Organization | Info-Tech Research Group