subrosa

A case study on how SubRosa assisted a global marketing agency in managing and assessing vendor risk

There is no denying that cybersecurity is a complex field and one that is multi-layered, third-party risk management is one of the most important aspects of ensuring comprehensive organizational security. As a result of increasing interconnectedness and globalization, third-party risk management is more critical than ever before. Notably, in recent times, third parties are becoming a major source of data breaches or are being targeted to initiate supply-chain attacks. Supply chain attacks pose a special threat as potential vulnerabilities on any one partner firm could be leveraged to infiltrate the main target and wreak havoc across the entire partner chain. Every linked partner firm could potentially open up many risk avenues. With multiple partner and vendor firms, the number of potential attack vectors and the overall risk increases manifold.

Introduction

The sheer scale of this threat makes combating it a difficult task. Most organizations are woefully underprepared or ill-prepared to effectively deal with this threat. Ensuring adequate data security and adherence to regulations outside the bounds of your organization makes vendor risk management a vast and complex process to initiate and manage. Tightened regulations mean that organizations are susceptible to be liable for the security controls and actions of their third-party vendors.

The SolarWinds attack which took place recently speaks volumes about the danger posed by supply-chain attacks. In this sophisticated attack, the attackers turned a seemingly run-of-the-mill update into a malware launchpad designed to target thousands of companies and government agencies worldwide. Over four hundred Fortune 500 companies and parts of the Pentagon, Centers for Disease Control and Prevention, the State Department, the Justice Department were all impacted. All by exploiting vulnerabilities in one particular firm.

The challenge

"We needed a cost-effective, efficient mechanism in place to manage vendor risk around both our existing and new suppliers. We are deeply concerned with the data management requirements that GDPR is requiring of businesses like ours and feel that such a program is a necessary step to take in order to maintain a competitive edge among enterprise clients, and more importantly, to protect our company and client data." *- our client, a global PR and marketing agency*

Being a global PR and marketing agency, our client had a heavy reliance on software companies and services partners. With clients and operations spread across the globe, our client also dealt with some of the largest Fortune 500 companies.

Under the latest regulations, companies that use consumer data are tasked with enforcing all rules listed under the General Data Protection Regulation (GDPR) throughout their network. Organizations are also required to convey their policies and procedures to their third-party partners and monitor proper compliance to ensure adequate data privacy and security. They must implement all the necessary measures to ensure GDPR-compliant data processing and have clear visibility into data flow and third-party data management. To this end, our client undertook a major initiative to secure data across their entire ecosystem of partner firms.

Vendor Risk Management

Vendor Risk Management is the act of assessing an entire supply-chain for cybersecurity risk and benchmarking, profiling and holding accountable all suppliers for their cybersecurity programs.

A properly run vendor risk management program will have the following expected outputs:

- Increased business resiliency through a hardened, security-conscious supply chain.
- An enhanced risk picture through the incorporation of vendor risk management in enterprise risk.
- A more effective supply-chain that works to improve your corporate security posture.

This vendor risk management project was an integral part of that initiative, one that was geared towards helping them achieve and maintain GDPR compliance.

The crux of the challenge:

- The biggest challenge was changing corporate culture. Prior to SubRosa working with them, employees would just install new software at will. This presents a great deal of risk as the company was unable to control the access of data and with which vendors their company and client data was residing with.

- The fact that the organization is very fragmented geographically and did not control new vendor onboarding prior to our engagement, made scoping them challenging. Also, the client organization had a broad vendor base geographically and many vendor partnerships were integral to key company operations.

- The firm did not have a standard procedure for conducting supplier risk management. Also, it did not have any tools or guidelines to gauge and manage supplier risk. The lack of a standard procedure to profile, organize and act on any vendor risks meant that all data and business-critical information of the organization was especially vulnerable to third-party risks.

To address this challenge, our client required a robust and scalable approach - a full, ground-up vendor risk management process built out to help assess risk for existing suppliers as well as when they procure or onboard new ones.

Our solution

Our in-depth risk assessment gave us a clear understanding of the client's needs.

After thoroughly scoping and assessing their vendor base, we analyzed the results to draft up the best solution to address this challenge. To gauge the scope of the vendor base, we worked with their finance teams to get an idea of accounts payable to existing suppliers and their procurement team to understand the existing processes for assessing new vendors, where applicable. This required a thorough examination of all third-party relationships and the scope of these relationships with regard to the data flow. Assessments were also conducted to gain a meticulous understanding of multiple external and internal data records and the nature of their sensitivity.

Due to the bespoke nature of the services, we had to custom build a robust program for the organization around their business goals, supplier base, and geographical location as they are multi-jurisdictional. Special focus was given to ensure that our client organization was afforded risk management ability across their entire vendor ecosystem in any potential scenario.

In order to ensure this, we undertook the following measures:

- Training the company personnel with a more focused and proactive cybersecurity approach to better deal with the onboarding of new vendors. Additionally, we built a central mechanism to control the onboarding process. This enabled one central team to track and alleviate vendor risk during the entire onboarding process.

- Building a vendor profiling questionnaire designed to give the organization a high-level understanding of each vendor's level of initial risk. With a clear evaluation of various surface-level risk parameters, it helps in identifying potential weaknesses at the earliest. The profiling questionnaire also helps the client gauge the level of vendor risk in-line with their organizational risk tolerances.

- Building a risk framework using NIST SP 800-30 guide for conducting risk assessment and the NIST cybersecurity framework (CSF) as the benchmark. The NIST SP 800-30 guide is widely considered as the gold standard for information security risk assessments.

The NIST 800-30 guide combined with NIST CSF helps in mitigating the likelihood of an attack as well as in remediating the effects of an attack, in case they occur.

- Risk-register and tracking methodologies were produced to enable the organization to track and coordinate with suppliers to remediate risks. With transparency and collaboration measures built-in, both the client organization and third parties can coordinate effectively to remediate any risks.

This multi-pronged approach was deemed to be the best fit for holistic vendor risk protection. At every step of the process, careful consideration was given to every potential risk vector and suitable measures were put in place to manage and remediate any threats in an effective manner. Constant monitoring and support ensure that third parties continue to adhere to the required standards.

Key insights

Our solution enabled the client organization to:

1

Have a clear picture and actionable input on vendor risk from all existing and new suppliers.

Have the ability to identify, evaluate and mitigate vendor risk across the board.

2

3

Have greater efficiency, effectiveness, and accountability in understanding the data flow outside the boundaries of its own organization.

The impact

In managing their vendor risk, the client can clearly understand where their sensitive data lies externally to their organization. With this ability to properly assess and understand the level of risk of all third parties, the organization now has increased confidence in its dealings with vendor firms. As mentioned previously, our client had a heavy reliance on software companies and service providers. They are now able to leverage these relationships for maximum benefit while being able to minimize the risk factor to a minimum.

The categorical process laid out by us which included profiling, organizing, and remediating of supplier risk level has provided our client with a step-by-step vendor risk management process. Additionally, their capabilities have been bolstered with the tools and procedures to tackle third-party risks of all degrees.

Our client has also seen improvements to both their internal enterprise risk program as well as supplier relations. Vendor risk management will not only allow them to assess and manage risk but also align themselves with suppliers who match their organizational security practices and mission as well.

With an effective vendor risk management process in place, they have ensured a consistent approach to data security compliance across their entire chain of partner firms. Enabling them to build trust and fuel long-term relationships that will bolster growth and partnership. Additionally, the processes and methodologies standardized as a part of this project will help them prevent supply chain breaches, and maintain overall compliance with GDPR while also minimizing corporate risk.

$15mn

Securing nearly $15mn of client data of some of the largest Fortune 500 companies

Approximately 40m data records were protected; including several sensitive records

Over 5000 passwords protected

Over 200 major brands' data protected

400 employees' HR data records secured, including medical and personal records