SECURITY ESSENTIALS (/BLOGS/SECURITY-ESSENTIALS/)

What is Third-Party Risk Management?

NOVEMBER 24, 2020 | MARK STONE (/BLOGS/AUTHOR/MARK-STONE)

Creating and maintaining relationships with third parties brings about multiple risks.

Whether your organization is large or small, it's almost certain that you have business relationships with many third parties for specific types of operations. When operational data and confidential information are exchanged with third parties, that data and information are vulnerable to misuse and exploitation. This is where risk comes into the equation.

When these third parties lack robust cybersecurity measures or compliance, building and maintaining a third-party risk management program is a crucial business decision.

The process of Third-Party Risk Management (TPRM) involves identifying, assessing and controlling all the various risks that can develop over the entire lifecycle of your relationships with third parties. TPRM often begins during procurement and should continue until the offboarding process is complete.

The big-picture potential risks are numerous, and can be reputational, strategic, managerial, and economical. More specific risks include data compromise, illegal use of information by third parties, the detrimental and damaging effects of non-compliance, and irregularities in supply chain management.

TPRM by the numbers

Still not convinced about the importance of TPRM? The numbers may change your mind.

For example, between 2018 and 2019, security breaches increased (https://www.accenture.com/us-en/insights/security/cost-cybercrime-study) by **11%, and 67%** since 2014. A 2020 Ponemon Institute report notes that over the past two years, 53% of organizations (https://www.forbes.com/sites/forbestechcouncil/2020/07/14/the-rise-of-third-party-digital-risk/?sh=45886e81480f) have experienced at least one third-party-caused data breach, with remediation costs averaging $7.5 million.

And here's what might be the most sobering statistic: According to a recent Osano report (https://www.osano.com/pr/privacy-breach-link) that observed the direct relationship between poor privacy practices and data breaches, the average American organization shares data with 730 distinct third-party vendors. Of those organizations hit with data breaches, third parties were responsible for two of every three.

When you add COVID-19 to the mix, third-party cybersecurity risk is even more of a concern for legal and compliance leaders.

Why is TPRM important?

Third-party risk management is a hot topic today. Just think about how the supply chain has changed for almost every organization, especially with the digital transformation in place to meet the needs of a changing workforce. Whether it's new cloud providers, new hosting providers, vendors or suppliers, there are many new companies with which we interact.

Even third parties you've done business with for years represent a security risk. Look at the infamous Target breach in 2013 — attackers were successful because an employee for Target's third-party HVAC vendor opened a phishing email and obtained credentials.

In this case, the HVAC vendor had more access to Target's networks than they needed. TPRM mitigates this risk. Plus, today, almost all compliance requirements outline the need for continuous monitoring of your third-party supply chain.

Let's face it: far too often, businesses decide to take their suppliers' word for it that yes, they are secure. Perhaps in many cases they are. But with so many vendors rotating in and out of our business, how do you manage access to your network or confidential data?

When it comes to TPRM, some common questions that you need to ask are as follows:

- What type of data are third parties accessing? What type of access?
- Have you given them physical access?
- What would happen if the third party's availability is compromised? How would that
- impact your business? What would happen?
- If they leak some of your confidential information, how would that impact you?

TPRM challenges to address and how to overcome them

Third-party risk management is not a process easily achieved in-house today. TRPM is a very resource-intensive task when you start to approach it manually.

Consider the challenges that are involved, including:

- Lack of resources
- Exhaustive list of third parties
- Multiple processes to evaluate
- Communication around issues
- Varying and numerous compliance requirements
- Constant change occurring for both parties
- Lack of workflow automation

Five steps to Third-Party Risk Management

No matter how you decide to address TPRM, there are five essential steps that will go a long way in minimizing risk.

1. **Identify** - The first step is determining which companies you do business with that could bring about any type of risk. An understanding of this third-party ecosystem is critical.

2. **Classify** - Taking a risk-based approach, you'll need to identify how much risk each third-party places on your organization based upon data, system access, and service provided.

3. **Assess** - Next, the security posture of the third parties you do business with must be evaluated. Depending on the nature of your organization, you'll have varying levels of assurance based upon third-party risk.

4. **Manage Risk** - Here, you'll outline steps to put policies in place and decide how remediation should be addressed. Basically, you're asking whether to accept or avoid risks.

5. **Monitor** - The last step involves the continuous monitoring of third parties to ensure they meet contractual obligations and sustain their security posture.

Why managed Third-party Risk Management services?

While TPRM can seem overwhelming, you don't have to tackle it all yourself. Many highly-qualified and professional companies can manage your TPRM program for you.

Depending on your organization, your TPRM needs will vary. You may only require a point in time assessment or a one-time report. Or, you may benefit from constant monitoring and flagging of problems detected in a third party's security posture.

Leveraging next-gen tools like FortifyData (https://www.fortifydata.com), managed TPRM takes people, processes and technology into account and can assess your third parties with a score that resembles a FICO credit score.

Going a step further, organizations can achieve optimal TPRM with TPRM-as-a-service (TPRMaaS). With TPRMaaS, all critical aspects of third-party risk management are handled by a team of experts.

They can help you:

- Manage third-party processes throughout the relationship lifecycle
- Onboard third-party companies
- Perform third-party risk profiles and categorization
- Provide third-party assessments
- Provide third-party oversight and manage workflow
- Present reports and continuous updates
- Provide ongoing monitoring of critical third parties

Do I really need to prioritize TPRM?

Yes, TPRM is complicated, and yes, given the ever-expanding threat landscape, it must be prioritized. Whether it appears near the top or the bottom of your priority list will depend on the number of companies you do business with that require some sort of access.

Your organization may have the most robust supply chain, but your overall security will only be as strong as the weakest link in that chain. Here's a great example that should help underscore the point: when you think of large companies like Apple, Amazon, Citi, Chase, Microsoft and Google, it's natural to assume they have a robust supply chain. But what if one of their suppliers suffered a data breach? This is exactly what happened (https://www.bleepingcomputer.com/news/security/massive-nitro-data-breach-impacts-microsoft-google-apple-more/) in October 2020, when approximately 13,772 accounts and 195,547 documents from these large companies were exposed after databases from Nitro Software were compromised.

Adding to the risk, ransomware (notably Ryuk) is escalating dramatically in 2020. The recent attack (https://www.cpomagazine.com/cyber-security/blackbaud-ransomware-demonstrates-the-potential-devastation-caused-by-supply-chain-attacks/) on cloud service provider Blackbaud should be cause for alarm. What if your vendors get ransomed?

Today, a robust cybersecurity posture encompasses much more than your employees, your hardware and software, and security tools. Any third-party tools or partners with access to your environment should be considered a critical component of your security hygiene.

(https://cybersecurity.att.com/blogs/author/mark-stone)

***About the Author:** Mark Stone*

Mark Stone is a content and copy writer with over a decade of experience covering technology, business, and cybersecurity. Earlier in his career, he was a cybersecurity analyst in the public sector. He lives in Kelowna, BC with his wife and two black cats.

Read more posts from Mark Stone › (/blogs/author/mark-stone)

TAGS:

‹ BACK TO ALL BLOGS (https://cybersecurity.att.com/blogs/security-essentials)

Search our blogs

Featured resources

INDUSTRY REPORT

Free trial (/products/managed-vulnerability-program/free-trial) **Get price (/products/manag**

AT&T Cybersecurity Insights™ Report:
5G and the Journey to the Edge (/resource-center/industry-reports/cybersecurity-insights-

report-tenth-edition)

Learn more (/resource-center/industry-reports/cybersecurity-insights-report-tenth-edition)

SELF ASSESSMENT

Benchmark your cybersecurity maturity (/resource-center/security-maturity-assessment?utm_internal=blog-rail-assess)

Explore (/resource-center/security-maturity-assessment?utm_internal=blog-rail-assess)

Free trial (/products/managed-vulnerability-program/trial)

Get price (/products/manag