BizzSecure
PEACE OF MIND FOR InfoSec

Vendor Risk Assessment

Table of Contents

Introduction

How do you know you are truly safe?

The world grows more complex by the day, and in this situation, secure is becoming one of the most coveted and yet difficult to achieve statuses. Needless to say, there is actually no way to ascertain whether your security armor is airtight or not.

Why is that? There are several answers to this question. For one thing, as businesses grow in stature, the number of security touchpoints increases, which naturally creates a greater attack surface for malicious actors.

Further, there's the question of technology: this is one aspect of modern life that is perhaps the most difficult to monitor. Technology changes by the minute, and what was once cutting edge becomes passé in a flash. Therefore, it is very difficult, and at the same time utterly essential to keep track of, and stay up to date with, the latest technological innovations. Technological advancements far out-pace the rate of human comprehension; due to this, new technology often renders existing security measures redundant.

Businesses today rely on digital infrastructure for their operation more than ever, and in this scenario, ensuring the safety and continued operation of an organization's digital assets is more important than ever. For this very reason, organizations are increasingly employing professional help to improve their internal security processes.

It must be remembered, however, that the business world is an interactive arena where no one can operate in isolation. In order to succeed in this playing field, one has to learn how to cooperate, coordinate and coexist with the other players in the fray.

As a result, organizations of significant stature often have to employ the help of external vendors to carry out specific operations on their behalf. This has multiple advantages in the form of responsibility sharing and cost benefits, not to mention gaining the advantage of third-party expertise in specific areas of operation.

But there's a flip side to this as well.

When working with third party vendors, it is extremely essential to determine that they conform with all safety and security regulations that the parent organization abides by. This is one of the prerequisites for a successful relationship of the vendor with the employer business.

Unless the vendors you are working with have the proper compliance settings in place, you are at risk of compromising the security of your organization by working with unsafe third parties. Therefore, before you start to work with a selected vendor, you need to ascertain yourself of the safety level of the vendor in question; this is a must if you want to ensure the continued safety of your organizational infrastructure.

…and also keep your company's reputation intact.

This is where Vendor Risk Assessment comes in. By evaluating all third parties that you choose to work with, the assessment process helps to guarantee that the vendors you have chosen to utilize follow all regulatory norms as required by your business. Even a single lapse on the part of the vendor can result in millions of dollars' worth of damage.

However, just conducting vendor risk assessment is not enough: it must be carried out in a thorough and correct manner. This is where many organizations fumble.

Vendor assessments traditionally have been, and still are, manual affairs that are conducted over phone. While this approach may work for small and mid-sized organizations with a limited number of vendors, when the number of vendors that you work with run in the thousands, such primitive methods of vendor risk assessment can become extremely cumbersome and virtually ineffective.

In such cases, modern methods of vendor assessment using the latest tools are a must to ensure the continued safety of your organization's assets. Proper vendor assessments by qualified professionals are a prerequisite for effective vendor selection.

In this eBook, we are going to delve deep into the diverse requirements that accompany successful vendor assessments; we are also going to take a look at the problems that organizations usually face while conducting vendor assessments, how the same can be overcome using modern tools, and what advantages can be gained through proper vendor assessments.

So, stick around; this is going to be an interesting ride.

To begin our journey, we have decided it best to go back to the basics and define exactly what vendor risk assessments are; so, let's start at the beginning.

What is Vendor Risk Assessment?

This naturally raises the question, who is a vendor? Put succinctly, a vendor is any third-party supplier who works with you as a partner in your business. This can range from raw-material suppliers, independent contractors to ancillary units that are working in tandem with your business.

Vendor risk assessment, then, is the method of evaluation that helps you to screen third-party suppliers in the act of selecting them as future business partners. The Vendor Risk Assessment Process works with the ultimate aim of identifying whether the vendor complies with all the security requirements that have been stipulated as essential by the parent organization.

This entire process is an important step towards ensuring the security of your digital assets. No matter the number of safeguards that you employ in your business internally, any security lapse on the part of an external player can seriously compromise the integrity of your infrastructure.

Therefore, it is essential that before you take on associations with any third-party organizations, you must verify their security credentials thoroughly. Otherwise you stand to leave some serious chinks in your security armor.

This is exactly what many organizations fail to implement properly. Due to reliance on traditional modes of vendor verification and assessment, these businesses fail to assess the multiple security parameters on which the intended third-party vendors should be judged.

This is mostly an outcome of an inertial tendency to stick to primitive routes for vendor assessment. As mentioned before, the entire process can quickly get out of hand once the number of vendors you associate with reaches a particular threshold.

Therefore, it is essential in the interests of your organization that you devote considerable time as well as up-to-date resources to ascertain whether your vendors are compatible with your security parameters.

Essential Criteria to Check During Vendor Risk Assessments

To ensure that your partners stick to your organizational guidelines and not compromise on the security of your assets in any manner it is of vital importance that you carry out a vendor risk assessment prior to taking on a business partner. This helps you to successfully analyze the vendor's work portfolio, and also to assess the risk levels of associating with the vendor, any red flags that their past history might raise, and also the likelihood of your assets being exposed to unwanted risks.

In the event that you are unable to conduct your vendor risk assessments in a coherent manner, you stand to put your entire organization in the path of security risks. This can lead to irreversibly damaging the reputation of your business, together with other unwanted outcomes such as legal sanctions, monetary losses and ultimately, the premature termination of your business entity.

These risks can be avoided by performing proper vendor risk assessments. But what are the prime factors on which vendors should be checked in order to ascertain their credibility and security levels? The following lists three such criteria on which you can assess your vendor's performance on the security front.

Background

Thorough background checks are essential in order to be certain of a vendor's credibility; before associating with the vendor in question, you must be sure of their ability to produce and supply high quality materials for your business; further they should be able to maintain this standard unwaveringly without putting your business and its patrons in any form of risk. By associating with a sub-par vendor, you risk putting your customers in a bad spot; this can reflect badly on your company and may eventually drive customers away.

Therefore, in order to avoid intense financial and reputational losses you must be sure of the vendor's ability to stick to the required security guidelines. This you can achieve by running proper background checks in the form of assessing reviews, taking note of prior customer feedback and also talking to the vendor's previous as well as existing clients. This will give you a clear idea of the vendor's work culture and past security history.

Compliance Adherence
One of the essential characteristics of a suitable vendor is that they stick to all regulatory compliances as required by your business. This is the first step to determining whether the vendor takes the appropriate care in handling confidential data.

Also, you should take careful note of the various security controls that have been put in place by the vendor and ascertain whether they align with those in practice in your organization. Mismatches should be immediately corrected through careful cooperation.

You should also take care to evaluate the vendor's response effectiveness in the case of a security breach; all this is relevant to keeping your organization safe from several security risks.

Documentation Practices
One of the characteristics of a vendor who adheres to a concrete security framework is the fact that they have all the necessary documentation in place. In case your vendor doesn't have the required paperwork in place that reflects their security credentials, it would be wise to steer clear of such partners.

The above three criteria form the essential pillar on which your vendor assessment should rest. However, don't think that you can start and stop your assessment after analysis of just these three points. Proper evaluation of vendors is a complex process that requires deeper insights and professional expertise to overcome the various barriers that you may face while performing the job, as the following will no doubt make clear.

Barriers to Effective Vendor Risk Assessments

Years ago, third-party risk assessments were considered a non-essential priority. In the wake of recent data breaches rooted in the lack of third-party compliance awareness, organizations all over the world have been jarred awake to the importance of vendor security ratification. Vendor security analysis is no longer a matter of minimal interest but rather one of prime priority. It is indeed a sign of positive change that organizations all over the world are waking up to the importance of vendor risk assessments.

As malicious players devise new methods of breaching organizations through third-party sources, vendors are in an ever-increasing risk of becoming the primary targets.

On the other hand, organizations are becoming more and more reliant on vendors for carrying out critical business operations, especially so in large enterprises. It is

understandable that without proper vendor risk assessments, organizations can put themselves at serious peril.

Recent research in this domain suggests that over 60% of data breaches can be linked to security lapses on the part of vendors, either explicitly or implicitly. The numbers themselves are proof enough of the risk improper vendor security measures can bring about in their wake.

Most organizations are seen to make the mistake of making internal compliance their top priority, thereby ignoring vendor assessments. While internal compliance is no doubt an essential part of your security plan, it really forms one side of the security coin. Vendor risk assessment is equally vital to your overall security plan.

The following are some of the essential barriers that organizations may face while carrying out vendor risk assessments.

Manual Methods

We've mentioned this before in this document once but think it wise to reiterate at this point: many organizations still carry out vendor risk assessments in the old-fashioned way, using manual methods such as telephone conversations. This, while sufficient in the past, is no longer adequate in the digital age.

Modern methods of vendor risk assessment demand the use of automated tools and analytical faculties to ascertain the viability of a third-party supplier. This improves third party assessment flexibility, introduces standard processes of assessment, and brings consistency in the reporting and documentation process.

The use of automated tools also improves the decision-making process and gives structure to the entire operation. It also introduces greater involvement of the vendors in the risk assessment process and contributes towards mitigating potential risks.

Such a standardized structure can be applied to all third-party suppliers. It also helps to optimize resources and streamlines the utilization of time as well as money.

Self-reported Questionnaires

Third party vendor assessments are usually carried out by means of questionnaires presented to the vendors, which they answer themselves. This approach is flawed in the sense that every vendor will necessarily highlight their positive points while glossing over the negatives. Therefore, it is essential to take the results of these reports with a grain of salt. Without disparaging the honesty of third parties you should always make sure to verify any findings reported in these documents.

Excessive Costs

Other methods that can be utilized for risk assessment are on site verifications and penetration testing of the vendors systems. While these are indeed more solid methods of assessment, they may be too resource intensive for certain organizations, requiring considerable amounts of time, money and human resources to be carried out effectively.

Outdated Data

The cyber-world operates at a very rapid pace, and it's hard to keep up with the changes. Often vendor assessments carried out in a particular point of time become outdated by the time that vendor is actually onboarded. So, make sure you always take updated data into account and perform the assessments within a reasonable time frame so as to render them effective.

These are only some of the many barriers that any organization may face while carrying out a vendor risk assessment. This topic itself is large enough to warrant a separate resource. Suffice to say that overcoming the above barriers is not easy, but they can be circumvented with a bit of planning and ingenuity.

Advantages of Vendor Risk Assessment

Now we have come to one of the most interesting parts of our discussion: why should we bother with vendor risk assessment at all? While it is clear from our exposition above that vendor risk assessment is vital to ensuring the security of your organization, the benefits of sticking to proper vendor assessment practices are manifold. Some of these are discussed below under separate headings.

Risk Reduction

The first and foremost benefit of a structured (and we cannot emphasize this enough: a structured approach is essential for risk assessment programs) vendor assessment is that it reduces the risk to an organization by a significant amount. While it can never be said that an organization is one hundred percent risk free, vendor assessments do reduce the chances of breaches by a significant amount.

Vendors who are working with your business, especially those that are in the practice of handling essential and confidential data, can put your organization in the path of severe breaches that lead to reputational as well as financial damage. Working with this dark cloud on the horizon should strictly be avoided. Proper vendor assessments can help you to assuage such risks and work with your vendors to derive the maximum value.

Improves Brand Image

Your customers are not going to differentiate between your internal security protocols and your vendor's security efforts. To them, your brand is representative of your business, and any security breach that may take place in your organization is bound to resonate negatively across your clientele.

By ensuring that your vendors stick to the right regulatory frameworks and taking the time to assess third-party providers before embarking on a business association, you stand to improve your brand image in the eyes of the world. As you reduce the likelihood of data breaches and other security incidents that can occur due to vendor oversight, you stand to create a brand image that is bound to hold stock with your patrons.

Increases Profits

This can be seen as a direct consequence of proper vendor risk assessment. If you associate yourself with the right vendors, this is bound to have a positive impact on your business operations. If your vendors ensure the correct security parameters across

their infrastructure, then this will be a boost to the security measures that you have placed in your organization internally.

This will naturally translate in mitigating security risks and losses due to security breaches; also, it will have a positive impact on the reputation of your business. This will organically bring in greater profits and reduce expenditure on correcting security lapses.

Reduces the Number of Vendors Required

This one, of course is an indirect consequence of proper vendor risk assessment. A thorough evaluation of your prospective vendors makes it easy for you to get a clear idea about the risk profile and competence of the vendor in question. By collating the data from these multiple assessments, you can easily create a vendor profile that will enable you to choose vendors based on their past records and safety standards.

By doing so, you can effectively reduce the number of vendors you actually need andby carefully choosing a few well placed, well experienced vendors who have the right security measures in place, you can create a manageable vendor pool from which to draw upon in times of need instead to wallowing through a sea of third-party providers.

Introduces Regulatory Discipline

Vendor risk assessments take the all-important step of introducing regulatory discipline across the organizational framework. By choosing to work only with vendors who adhere to the strictest regulatory standards, you stand to create a culture of security discipline that is essential for the smooth and secure functioning of any business. Further it creates a sense of safety among your internal employees as well, who can be sure that their efforts will not be hampered due to any laxity on the part of third-party players associated with your business.

Enables Synergistic Partnerships

Efficient vendors can contribute to the success of an organization on a large scale. Certain vendors are able to associate with large organizations on a level more advanced than that usually offered by regular third parties. A thorough security assessment facilitates the process of establishing trust between the business and the vendor.

This can lead to long lasting synergistic partnerships that operate effectively as as single functional unit. As vendors and organizations continue to work over extended time periods, the understanding and relationship between them evolves into something more than mere functional efficiency. As the companies already have a shared basis of trust, conflict resolution becomes simpler and speedier.

Formulation of Shared Goals

Proper risk assessment builds confidence between business partners, leading to the formulation of shared goals in terms of security management.

The creation of shared goals can contribute towards the effective collaboration between your business and your vendors.

Helps You to Gain a Comprehensive Risk Picture

This needs a bit of explaining. As you go about conducting risk assessments for a large number of vendors, this can actually reveal keen insights regarding the various risks that your organization may face from associating with unsafe vendors. This will give you a clear idea of the quarters from which your business may be threatened. Each time you perform a successful risk assessment you stand to gain knowledge that can further improve your next assessment.

Apart from the above, risk assessment of a vendor also provides you with a framework to perform in-house risk assessments of your own business. Of course, all this will be possible only when the vendor risk assessment is carried out according to professional guidelines.

Create a Vendor Database

Continuous and comprehensive vendor assessments will help you to build up a database of vendors along with corresponding risk metrics. This can enable you to compare risk scores between competing vendors and provide you with a streamlined system of metrics for evaluating vendor risk levels.

This can not only help during the initial vendor selection, but also can be put to use for vendor recompetes and contract renewals. A database of low-risk vendors with updated risk scores empowers your organization to associate with those third-party providers who have an established track record of implementing strong security controls and data protection mechanisms. This can actually reduce the time and cost required to acquire vendors.

Gives You Leverage Over Your Vendors

Employing a vendor naturally involves negotiations, and there may be multiple businesses vying for the same contract. If you have a clear notion about the risk profile of a vendor, then this gives you a certain amount of leverage which helps you to negotiate better. In some cases, you can even compel the vendor to comply with your requirements.

This may also provide you with a tool for monetary negotiations. This has the effect of reducing the cost of acquiring and maintaining vendor relationships. All of this ultimately contributes to improved vendor conduct and has a significant positive effect on your business.

Introduces Organizational Consistency

Vendor risk assessment is an activity that should not necessarily be restricted to the person or team responsible for performing the assessment. Instead, vendor risk assessment must be understood consistently by the entire organization. The entire process must be structured in such a way that even if there are leadership changes, the new entrants can easily carry on the task of their predecessors without interruption.

Further, an organization wide understanding of vendor profiles helps individual departments to engage vendors without needing to go through unnecessary corporate red-tape. For larger organizations with portfolio companies or multiple brands, this can translate into massively efficient processing. Such a centralized nature of risk assessment allows your business to operate fast and without interruption.

Improves Vendor Quality
Finally, perhaps the most prominent benefit of employing proper vendor risk assessment is the fact that this will improve the quality of service that you receive from your vendor partners. As you continue to work with service providers who are in line with your security policies your organization begins to reap the benefits of superior service and effortless partnership.

The above benefits are certainly the top advantages of carrying out a streamlined vendor risk assessment. Remember though, that this is only the tip of the advantage iceberg.

Yet, in spite of so many benefits, there may still be some organizations which balk at carrying out vendor risk assessments, solely to save on a few dollars. For those of you who are still apprehensive of spending on vendor risk assessments, the following argument may sway you to the other side.

Why Should You Invest in Vendor Risk Assessments?

Unless you are a special kind of business that takes pride in staying small, you are looking to scale up fast and in a secure manner. In order to achieve this end, creating a solid framework for vendor risk assessment is one of the best steps that you can take.

The benefits are obvious as explained in the above section. Apart from this, a vendor risk assessment program provides you a significant return on your initial investment. Whether it's in the form of savings resulting from vendor fees negotiations, savings in the form of reduced loss due to security breaches or greater levels customer acquisition, vendor risk assessments are one aspect of your business that you cannot, and should not, ignore.

Vendor Risk Assessment Best Practices

As with everything, vendor risk assessment needs to be done in a structured (again!) manner. The following are some best practices that you can adhere to when performing the assessments.

Don't Overlook
If you are a large organization that employs thousands of vendors, it can become very difficult to keep track of all of them manually. In such a situation make sure that your vendor assessment program is automated and provided with the latest vendor data. This way you won't overlook a vendor when performing risk assessments. Although smaller organizations with fewer number of vendors may not necessarily face this problem, it doesn't hurt to employ the latest methods... which brings us to our next point.

Leverage Technology

We are currently living in the era of technological revolution. Every moment, disruptive technologies are being born that hold the potential to upend the status quo. Organizations should certainly take advantage of this and leverage the latest technologies to streamline their vendor risk assessment process.

From assessment automation to incorporating machine learning in the data analytics process, technology holds the key to a better vendor risk assessment process. Therefore, your organization should not delay in reaping the benefits of the latest and greatest in terms of tech.

Segregate and Control

One of the most efficient techniques that you can use in order to effectively manage your vendor risk assessment program is to segregate the potentials into different categories based on the type of service they provide. Then, carry out the risk assessment for each vendor in every category, and classify them on the basis of their risk scores. The vendors with the best score from each category should then be selected.

This approach follows the age-old algorithm of divide and conquer: by separating each vendor into different brackets, you can effectively realize which are the ones that you should choose, and which ones to leave.

Further, you can also classify and group vendors according to the impact that their association might have on your business; they can be classified as critical or non-critical vendors.

Be Repeatable

Keep in mind the fact that vendor risk assessment should be a repeatable process, not a one-and-done affair. You should formulate your assessment plans in a manner that is consistent with the security policies and procedures practiced in your organization.

This means envisioning a framework for risk assessment that can be repeatedly applied, updated, and scaled according to your organizational needs.

Perform Product/Service Level Assessment

Along with focusing the risk assessment procedures on individual vendors as a whole, you should also consider performing a product/service level assessment of each vendor. This can help to determine the impact that association with that vendor will have on your products/services.

Do Your Due Diligence

Never take a lackadaisical approach to vendor risk assessment. Always be sure to perform your assessment activities diligently and with utmost professional integrity. Taking care while performing the assessment of vendor risks can pay off significantly in the long run as monetary as well as time savings.

Be Updated

This is a very essential point. Of course, we don't mean to say that the other points are not important, but this one holds special significance. Regulatory requirements and compliance rules change over time. As a result, risk assessments cannot be static

activities and must change with the requirements. As a business, your organization must be aware of the latest compliance and regulatory changes that are applicable to you, and you must be ready to incorporate the same in your vendor risk assessment strategy.

Keep Management in Mind
While you conduct a vendor risk assessment, make sure that top level management is always informed of any changes, updates or outcomes of your assessments. This keep the top executives in the loop, and guarantee their continued participation and help, which is crucial for the success of your risk assessment plans.

Rope in the Professionals
Finally, in case you find the entire vendor risk assessment process too cumbersome and time consuming, you can always employ the help of professionals who are experts in such assessments. Taking the help of experts can help you to lighten the load off your shoulders and instead focus on your core business functions.

Keeping these tips in mind can help you to lay down a solid base for your vendor risk assessment program.

Conclusion

Creation of this document has truly been an undertaking, and we hope that it has been informational for you as well. After such a long discourse on a single topic, heads are bound to reel slightly.

Fear not. Vendor risk assessments are not something to be afraid of. Rather they are an essential part of the vendor selection process. It's true, that some organizations can think of the entire process as unnecessary and choose to go with vendors they have traditionally worked with. While this may work for small organizations, it is no doubt a bad idea for any organization of considerable scope.

The business landscape of the 21st century is ever changing and morphing into complex systems that were unheard of previously. In this situation, organizations cannot ignore the importance of working with the right partners.

Businesses cannot operate in isolation; they need to collaborate and coordinate with each other to create a synergistic environment where everyone can mutually benefit. In this light, vendors play a very important role. Third-party suppliers not only aid the functioning of a larger organization, they create opportunities for strategic partnerships which can open doors previously unseen.

Therefore, no organization of significance can hope to operate without associating with third party players.

Nevertheless, it must be kept in mind that vendors provide a very attractive attack surface for malicious agents. As many vendors are small operators which have to make do on a tight budget, they may not always have the required resources to be security

complaint on all fronts. This is a vulnerability that cyber criminals are always quick to explore and exploit.

Therefore, organizations working with vendors must implement adequate vendor risk assessment programs to evaluate third party suppliers for security risks. This is one of the essential prerequisites to ensuring the continued safety of your organization's digital assets.

So, the next time you have to implement a vendor risk assessment, keep the teachings of this resource in mind. We are sure that you will benefit from following the discussions laid down in these pages.

However, if even after this you feel that you do not have enough time or resources to conduct your vendor risk assessment on your own, remember to employ the help of experts who are adept in this task.

After all, two heads are always better than one.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com