BizzSecure
PEACE OF MIND FOR InfoSec

Integration of Vendor Risks and Remediation

Table of Contents

Introduction

Cyber-threats are always evolving in this digital age. No matter what kind of data your organization deals with daily, it is crucial to protect it from such intelligent cyber-threats. This is easier to do when you and your organization are the only ones in charge of ensuring the protection of your digital assets. Unfortunately, businesses revolving around the digital world are seldom in this position.

There is typically an involvement of one or more third-party organizations or vendors. These third-party vendors could be helping your business in any number of ways. They may be providing you a security service to prevent data loss through malicious hackers. They could be helping you with conducting financial transactions with your customers.

Third-party vendors bring with them expertise that can help your organization grow without having to spend heftily on training your own employees or hiring new ones, for such tasks. Thus, they help you increase the efficiency and cost-effectiveness of your organization. Such benefits do not come without risks.

As the number of vendors that you share your data with increases, the number, and threat-level of the security risks you are exposing your organization to also elevates. As data security risks increase, the likelihood of sensitive employee or customer data being leaked, lost or misused also rises. This can gravely jeopardize your organization and its customers.

The gravity of leakage or loss of people's confidential or sensitive personal information is an issue that the government also takes very seriously… and for good reason. Data breaches can cause immense damage to people's personal data related to their social security, finances, health, and other important aspects of their daily lives. Securing the country's digital assets is also important for national security efforts. Therefore, it is not surprising that several federal and state laws are in place to protect people's digital information.

For example, the Gramm-Leach-Bliley Act or GLBA regulates how customers' private information is shared and secured by financial institutions. Additionally, businesses involving storage, processing or transmission of credit card data of customers must stringently follow the Payment Card Industry (PCI) Data Security Standards (DSS). Similarly, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was formulated to protect the healthcare data of patients from misuse and fraud. Some state laws like the California Consumer Privacy Act (CCPA) also helps to regulate businesses.

In all these and many other cases, non-compliance or poor compliance with these federal regulations could mean irreparable data loss or leakage, substantial monetary penalties, and legal action as well. Therefore, if your business is regulated by such federal laws that necessitate flawless protection of your customers' digital assets, you must invest time, energy and money in ensuring risk assessment, compliance, and remediation. When we say risk assessment, compliance or remediation, we mean that these tasks need to be performed not just by your organization, but by your vendors as well. This is because any error on part of your vendors will cause financial and legal damage to your business as well as the vendors. This makes vendor risk assessment and

remediation a collaborative process that requires a healthy back and forth of data, regulatory information, and remediation plans between your organization and the vendors.

This book will make an interesting and important read for both business-owners and the vendors that help them conduct their business operations. We discuss the basic types of vendors that organizations typically interact with, the risks they pose and the key performance indicators (KPIs) one must look at to properly evaluate these vendors. We also shed light on how to perform vendor risk assessment, what remediation means, and why and how one should integrate vendor risks and remediation. In the end, we also provide our suggestions on how to minimize vendor risks in the future so that your organization requires minimal remediation efforts and resources.

Vendors and the Risks They Pose

Any organization typically requires multiple third-party vendors who help them smoothly conduct their business operations. However, a single missed data breach or intrusion caused knowingly or unknowingly by a vendor can bring your operations crumbling to the floor. Let us look at who these vendors are and what kind of risks they pose to your organization.

Depending on the kind of business you are in, your vendor requirements would differ. There could be vendors who help you manage the devices in your organization. Some would manage the network services by fulfilling your internet or local area network requirements, while others could be providing your organization with cloud services for data storage and sharing. Some would be actively involved in helping you secure your data assets, such as antivirus or antimalware software providers. There could be vendors that process your employees' or customers' data to help with the credit card or other financial transactions.

Whatever is the nature of your data transactions with your vendors, you are constantly exposing your organization's framework to vendor-related risks of varying intensities. Here are some of the risks which the vendors assisting you in your business can pose:

Compliance

Complying with the various regulations pertaining to consumer data is a difficult task as it is. When it comes to a third-party vendor, you can never be too careful. Even if you are perfectly compliant in all your business operations, your vendor may not be. Assuming that your vendors are compliant can be a huge mistake.

Data encryption and access

Trusting a third-party is the issue at heart when talking about vendor risks. If you need to share your organization's data with a vendor for some downstream processing, a massive risk is: do they encrypt your data? Another risk factor is the number of people in their organization who have authorized access to your data.

Reputation risk

Your organization is always going to be the face of all its business operations, even if some of them are outsourced to third-party vendors. Your customers trust you to securely collect or process

their data. Any security lapses caused by a vendor will bring you to the forefront of the error propagation chain. The first thing that happens in such scenarios is the loss of trust of your customers. Your organization's entire reputation is at stake when trust is lost. This is a major risk of third-party vendors.

Financial risk

You are, of course, exposing your organization to potential financial risks when you hire a vendor to take care of your data in any way. The financial risks may be associated with inadequate security measures by the vendor, or with the vendor not being able to continue their end of the service due to non-compliance or financial issues. In either case, your organization is risking its business continuity. Financial risks become particularly dangerous when credit card, insurance, tax, or other financial information pertaining to your employees or your customers is required to be shared with your vendors.

Unfamiliarity with regulations

If you and your vendor operate from different countries, an important requirement to keep in mind is ensuring compliance with the laws of the other country. Compliance is required both from your organization and the vendor. In the absence of physical proximity to the region of operation, compliance with regulations could be an issue. This could stem from insufficient knowledge of regulations in the other country or location, or simply due to communication gaps. Another risk is that you may not get to completely understand the functioning of your vendor if they are based in a separate country. In fact, even within the country, regulations concerning your business operations may change from one state to the other. If your vendor is in a separate state, unfamiliarity with your regulations is a risk that is always going to bother you. This becomes particularly prominent if the vendor you are looking to hire is a small organization limited to a single state.

How to Perform Vendor Risk Assessment?

Information security risk assessments are an important and premier part of any information security policy design task. Vendor risks must be assessed regularly in a similar manner. Now that we have taken a closer look at the kind of risks vendors can expose your organization to, how do we assess new and existing vendors for the likelihood of these risks? What follows are the steps involved in a vendor risk assessment.

Create a list of all vendors

Enlist all the vendors that support your business operations in one way or the other. Do not consider the scale of operations when drafting this list. This first list should be exhaustive. It should include each and every vendor that helps your organization by generating, storing, securing, sharing, or processing your data among other tasks. Once you have created this vendor database or a portfolio, the next steps become organic for any organization.

Understand how your vendors use your data

Ensure that you know and understand how each of the identified vendors affects your business. This involves knowing what data they have access to, what they do with the data provided to them, and how careful they are with that data. This could be a make-or-break step for the indispensable task of vendor risk assessment. If you are unaware of what a vendor does for you and how exactly they use your organization's data, you will not be able to continue with the next steps in a vendor risk assessment.

Categorize all vendors based on associated risks

Based on your knowledge of all vendors and the risks associated with them, you must classify the vendors as 'low-risk,' 'moderate-risk,' or 'high-risk' vendors. You may even use more detailed risk classifications. For instance, a certain vendor may be associated with a 'financial risk,, while another may be posing a 'reputational risk.' There could be 'regulatory or compliance risks' as well. Another system of classification that you could follow is based on the kind and fraction of your organization's data that is shared with a vendor. For example, some vendors may simply be providing you with hardware and devices such as external hard drives or servers for your data. These vendors would be primarily responsible for your data storage. Others may be responsible for data maintenance on industry software. Yet others may be involved in both of these aspects simultaneously. Depending on your business, you will have to come up with relevant risk categories to better understand how your vendors may threaten your security posture. You can also use KPIs to classify your vendors. Some important KPIs to watch out for are described in the next section.

Think of a remediation plan

The actions your organization must take to remediate these risks must also be designed, compiled, and elaborated during the vendor risk assessment. This will help you link the vendor risks and their risk-levels with the kind of action you must take to remediate them. A major advantage of this integration is that it makes it easier for you to perform remediation in the future. We will discuss this point in greater detail in the upcoming chapters.

In order to integrate vendor risks and remediation, vendor risk assessment is a must-do first step. Remember, it is never too late to start a thorough vendor risk assessment for your organization.

Key Performance Indicators (KPIs) for All Vendors

We have already established that all the vendors involved with your organization must be assessed for risks and audited regularly. However, what are the indicators that tell you that you chose your vendors wisely? How can you tell if you need to rethink your contract with a certain vendor? KPIs can help you answer all these questions. They can also help you rate and classify your vendors into risk categories when you perform a vendor risk assessment. Here are some of the KPIs you should consider tracking for all vendors.

Quality of work

As expected, this is one of the most important KPIs to track vendor performance. What kind of operational issues are caused in a task assigned to a vendor? Does the vendor prioritize addressing those operational issues for your organization? In some cases, customer feedback provided to your organization may also be directly or indirectly linked to an operation performed by a third-party vendor. Are the customers satisfied with the products or services being supplied to them? The answers to such questions give you an idea of the quality of work being done by your vendors.

Compliance

We have already suggested that one must perform regular vendor audits to track compliance. These audits are essential indicators of the vendor's performance. If the vendor is always compliant with federal and state laws, it is a good start. Further, any vendor dealing with your organization's data must also follow your own information security and compliance policy stringently. An excellent compliance record also indicates that your vendors conduct good internal audits to ensure immaculate information security. A good rating on this KPI means that your organization's operations are in good hands.

Innovation and Improvements

In the complex and changing world of cyber-security, one cannot risk being complacent. Innovation and improvements are necessary to keep up with new data security threats that present themselves. If your vendors provide suggestions on how to improve your security posture or save operational costs or improve efficiency in general, they have your best interests in mind. An innovative and self-evaluating attitude suggests that your vendors are keeping an eye on the developments in the cyber-security world. Such vendors should be rated highly.

Remediation efforts

Remediation efforts are of paramount importance when a threat becomes live. If one of your vendors is responsible for exposing your organization to dangerous risks, it should be their top priority to help with the remediation of those risks. All risks that need to be remediated must be dealt with completely and in a timely manner. Time lost is equivalent to actively distributing confidential data to network intruders. Nothing could be more harmful to your business and your clients. To ensure timeliness in remediation efforts, the vendors must have an efficient remediation plan at hand. Rate your vendors on their eagerness and preparedness to deliver remediation.

Communication

In order to help your organization in its business operations, any vendor needs to be active in communicating its requirements from you. They should keep you up to date on what customer or employee data needs to be shared with them, and how they are processing or storing that data. They need to be responsive to the vendor risk assessment reports that you send to them for review and remedial action. They should also provide you updates on their internal risk assessments and

compliance so that you can trust them to handle their data. All these require impeccable communication from your vendors, making it an important KPI to track.

These and many other KPIs should be constantly tracked to rank and assess your vendors for the risks they pose to your organization.

What Does Remediation Entail?

Let us say that despite your best efforts to ensure that your vendors are risk-free, a vendor-related security breach occurs. This is not an unrealistic scenario as data suggest that a lot of network security breaches and threats are linked to third party vendors. In such an event, instead of panicking, you must immediately start implementing the contingency plan you have prepared beforehand: remediation. Remediation is a combined effort between your organization and the vendor(s) that caused the security breach.

Formulate a remediation plan

Yes, we know that we had included this as one of the steps under 'vendor risk assessment' as well. This is how closely the tasks of vendor risk assessment and remediation need to operate. Formulating a remediation plan in advance is necessary to ensure that risks can be mitigated efficiently when the time comes. Remediation plans must be customized to each business-vendor relationship. The plan needs to be prepared in a collaborative way so inputs from both parties are incorporated.

Since your organization is likely to have more than one vendor, you should also assign priorities to the vendors based on the risks to which they are linked. Prioritizing becomes particularly important when a given security threat is a result of errors propagated through two or more vendors. In such cases, adding priorities to your organization's remediation efforts will make the entire process more efficient.

Communicate your remediation needs

In the unfortunate event of an information security threat becoming a reality due to a lapse at your vendor's end, communication gains supreme importance. Details of the compromised data and further associated risks identified must be communicated and shared immediately, effectively, and transparently to each vendor. In fact, to ensure proper remediation, even your reports of vendor risk assessment should be sent out to the concerned vendors so they can propose useful remediation measures. It will also make the vendors more compliant in general.

Enforce accountability

Accountability is indispensable. When it comes to remediation, each vendor must be accountable. No matter what a vendor's status or business relationship history with you is, they all need to be treated the same way. Bias will lead to a lack of accountability from vendors. Therefore, when you communicate your remediation needs to your vendors, follow-up with them to ensure that they remain accountable for their mistakes.

Hire an impartial third-party

On paper, remediation may seem like an easy task to perform. However, there could be times when your organization and the vendors are unable to effectively take remedial measures to contain a threat. An important reason why remediation measures fail is playing the blame-game. Authorities often tend to blame each other for risk exposure, especially when it comes to multiple vendors. In such situations, the remediation process can be a cooperative one. This means that you can work in conjunction with third-party vendors as well as hire more experts in the area that needs remediation. Experts will be impartial in such situations and instead of blaming your organization or any of the vendors, they will focus on the task at hand.

Why is Integrating Vendor Risks and Remediation Important?

Preparedness in the event of a disaster is of utmost importance. This applies to impending vendor risks as well. If and when your organization becomes vulnerable to a vendor-associated risk, the timeline of remediation efforts is vital. You want remediation to be quick and efficient. Additionally, to ensure speedy remediation, the allocation of the right resources is a crucial task as well. One way to make certain that remediation happens immediately in the event of a vendor-related threat or exposure is to integrate vendor risks and remediation.

Integrating vendor risks and remediation makes all the aspects of information security and compliance, including vendor risk assessment and risk mitigation, extremely judicious and efficient. It also reduces the number of employees required to divert their attention to remediation when they can be working on other assignments that require their attention. The integration of these aspects also eases keeping track of all the ongoing and required remediation efforts. You can keep an eye on whether remediation is being done in a timely manner and if the resources are being utilized in the right way. You can also immediately generate reports on the extent and quality of remediation efforts at any given time, in case you need to present them to your organization's board of directors or other authorities.

These benefits of integrating vendor risks with remediation make it useful for organizations and vendors alike.

How to Integrate Vendor Risks and Remediation?

To better perform the tasks of vendor risk assessment and remediation, a highly effective measure is to integrate vendor risks and remediation. We have already highlighted this and other needs to integrate vendor risks and remediation in the previous section. The question, then, is how to integrate the two? Here are some steps you should follow to integrate vendor risks and remediation.

Make integration a part of vendor risk assessment

As we have discussed before, both vendor risk assessment and remediation require you to design an efficient remediation plan. If you incorporate a remediation measure beside any and every risk that you identify in your vendor risk assessment, integration of vendor risks and remediation will happen organically. This becomes even more important when you have multiple vendors working for your organization. In such cases, you should make use of the risk-based classification of

vendors that you utilized for the earlier risk assessment. based on the risk category, you can fix a remediation measure for any given vendor risk.

Collaborate with your vendors on organizational remediation policies

If vendor risks assessment and remediation are not collaborative in your organization now, we would strongly advise you to make them such with both old and new vendors. This greatly increases transparency and trust between your organization and your vendors. Apart from these benefits, it makes the merger of vendor risks and remediation an easy task.

When you design your remediation plan using your vendor's inputs on their threat mitigation capabilities, you can better understand how a potential risk can be addressed by the vendor. This way, you can directly correlate and assign a remediation step to a previously identified vendor risk. It also means that your vendor will now know what risks you have associated with them and the remediation that you expect from them in the event of a threat.

Keep track of your vendors' remediation efforts

An important step in integrating vendor risks and remediation is to monitor how well your vendors are performing their end of the remediation task. If during this assessment, you find that a certain risk is not contained by the previously set remediation measures, you can immediately update the remediation plan for that risk. This link between vendor risks and remediation is exactly what you should seek to make your organization more secure and prepared.

Reassess the remediated risks

Reassessment of remediated security risks is an often-overlooked part of integrating vendor risks and remediation efforts. A reassessment will help you identify any other loopholes in security efforts. It will also help you evaluate how well you and your vendors' information security policies have developed or matured over time.

Automation is the way to go

The integration of vendor risks and remediation is a task that requires dedicated resources and time. To perform a vendor risk assessment and remediation manually, you must appoint a set of employees to assess the risks associated with each vendor of interest. The appointed employees would then:

1. Perform vendor risk assessments following the steps we described previously.
2. Submit vendor risk assessment reports to the authorities in your organization as well as to the respective vendors.
3. Communicate the remediation requirements of the authorities in your organization to the authorities in your vendor's organization.
4. Follow up with the remediation efforts internally in your organization.
5. Keep track of what the third-party vendors are doing at their end to fulfill your remediation requirements.

As expected, it does get tedious if done manually. This not only consumes time but also financial and personnel resources. It might also make your organization less effective if the same employees are involved in maintaining your key business operations while also manually keeping track of vendor risks and remediation.

If you do not want to engage your own employees to do these tasks, you can hire a third-party organization to perform the risk assessment and remediation planning for you. This will also be better than asking your own employees to perform the task because it will provide an unbiased and more transparent view of the risks associated with any vendor.

However, as long as these aspects of your relationship with your vendors remain manual, risk assessment and remediation can be expected to be tedious and prone to mistakes. Thus, the integration of vendor risks and remediation is best achieved through automation.

You can automate both vendor risk assessment and remediation. The automation of the vendor assessment process makes it more transparent. This will help you save the time and money invested in the assessment. It will also help you ensure consistency, set vendor standards for your future needs and perform a real-time risk assessment. As we have discussed before, for integration, once you have your risks assessed, they need to be communicated to the vendor so that you can come up with a remediation plan together.

Automation allows you to directly send your vendor risk assessment to the concerned vendor. Once the vendors receive their respective assessments, they can start working on the remediation plan immediately. The progress of their remediation efforts can be monitored in real-time by your organization. Automation also gives you the necessary visibility of how far along you are in the remediation efforts. It allows you to compare one progress assessment with any previously conducted assessments. This shows you the overall progress in your organization's security and remediation efforts over the years.

An important benefit of automation is that it lets you look at all the vendors, the associated risks, and the progress of their remediation efforts on one single software platform. This makes it easier for you to present real-time vendor risk assessment and remediation data to your stakeholders.

Considering the numerous benefits of automating vendor risk assessment and remediation, you can easily integrate vendor risks and remediation for your organization. Follow our steps for integrating these two aspects and make vendor risk assessment and remediation easier for both your organization and your vendors.

How to Minimize Vendor Risks in the Future?

So, you have performed an intensive vendor risk assessment for your organization and integrated the risks with remediation. What is next? Is there a way to minimize future risks when hiring new vendors so that minimal remediation efforts are required? Indeed, there is. Especially now, when you have an in-depth idea of all your vendors and the risks they may pose to your organization.

Here are a few things you must ensure before you hire a new vendor.

Set vendor standards

One thing which can save you a lot of effort in the future is to set your vendor standards. Your ongoing vendor risk assessment will be based on all the vendors that are currently helping in your business operations. However, once this step is done, you can set standards for any new vendor that your organization may need in the future.

Verify that new vendors will meet your standards

Now that you have set good vendor standards for your business operations, evaluate all potential vendors based on these standards. Your organization's vendor risk assessment will provide you insights into how to ensure that new vendors meet your standards. The key thing to remember is that you are looking for a vendor that poses the least risk with the best history of KPIs. We have already discussed KPIs in detail in a previous section.

Request a detailed remediation plan

Your vendors should be able to provide and discuss with you their detailed remediation plan in case a potential risk becomes imminent. We have already discussed how vendor risk assessment and remediation are collaborative steps. When hiring a new vendor, you need to know that in a vulnerable situation that endangers your organization's data assets, your vendor will help you out with a well-laid remediation plan in place.

Monitor their activities related to your organization

Your vendors should allow you to freely monitor their activities related to your organization, because in the end, what they do has a massive impact on your organization's business operations. Even when they are conducting remediation steps, your organization should have the authority to monitor their actions and suggest changes that best suit your operations at the time. This aspect must be included in your organization's contracts with each of your vendors. You can either assign this task to an existing employee or hire someone specifically for this task.

Ask for regular updates on remediation

Your vendors should be willing to provide you frequent, regular updates on the remediation policy and efforts. Typically, as we have mentioned several times now, remediation should be a collaborative action. If your vendor risks and remediation are integrated with an automated fashion, monitoring the updates on remediation would not be difficult at all.

Regular and frequent assessment of all your vendors

Even if you have chosen your vendors with the utmost care and you have great confidence in them, you must perform regular and frequent assessments of their performance. Use the various KPIs that we have discussed earlier and make your assessment visible to all your vendors so that they can take the necessary actions to improve themselves. If this is done frequently, major loopholes in security measures can be detected and resolved immediately.

Conclusion

The give and take between vendors and IT are almost impossible to completely avoid any vendor risks when doing business. However, there are countless ways in which you can alleviate a large proportion of the highly damaging vendor risks and be prepared to mitigate the rest.

Your job is half done if you choose the right vendors. Choosing the right vendor requires you to consider what they do for your organization, the risks they pose, and their KPIs. In the end, your choice of vendors should align with your overall objective of protecting your customers' and employees' data.

If a risk does befall your organization on account of one or more of your vendors, you and your vendors can still remediate the threats. Hopefully, we made it clear that remediation is by no means a solo task. It requires conscious and continuous collaboration with the vendors that pose risk to your organization. Hence, it is important that the necessity of integrating vendors risks and remediation efforts be shared and discussed with all involved stakeholders.

Overall, we hope that this book could successfully explain to you both the need and the means for integrating vendor risks with remediation. We have attempted to summarize all these aspects of vendor evaluation, risk assessment, and remediation in this book. Follow our steps for vendor risk assessment and remediation so you can take your organization miles ahead on the road to information security.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com