BizzSecure
PEACE OF MIND FOR InfoSec

How to Manage Vendor Risks

Table of Contents

Introduction 3
What Risks Do Vendors Pose? 4
Vendor Risk Assessment 6
Preventing Vendor Risks 7
Vendor Risk Remediation 9
Integrating Vendor Risks with Remediation 12
Automation of Vendor Risk Management with the EAID Solution 14
Conclusion 16

Introduction

Organizations with vast business operations heavily depend on the expertise of third-party vendors to conduct different tasks. They could be involved in developing security systems such as antivirus software or intrusion detection systems, manufacturing data storage devices such as external hard disks, processing data, enabling financial transactions, and other such indispensable tasks.

Third-party vendors can certainly increase the efficacy of your business operations. However, they are also the biggest source of risk in all organizations around the world. This is because the control of your organization on the operations of third-party vendors is minimal if not zero. Moreover, the visibility of their ways of processing or handling the data that you share with them is also extremely poor.

These disadvantages escalate when there are more vendors working for your organization. Mismanagement of vendors can add to the risks they pose to your organization's security and business continuity. Such risks can lead to loss, leakage, or misuse of sensitive and confidential customer data by malicious actors, which can lead to loss of trust, reputation, customers, and money and could even result in lawsuits by customers and regulatory bodies.

In this book, we have described the different ways in which you can manage vendor risks in your organization – risk prevention and risk remediation. Let us first understand what risks vendors pose and how you can assess them in your organization.

What Risks Do Vendors Pose?

Third-party vendors are the most prevalent risk factor in the world of digital information. While they are indispensable to the functioning of organizations, they are not in the direct control of the clients they assist. Information security risks that arise from the organizations of third-party vendors are likely to go unnoticed by the clients.

What are the risks that third-party vendors pose? Let us take a look.

Tracking compliance

Third-party vendors are hired by different organizations for various purposes. If they are directly handling the data that you obtain from your customers (or even employees), compliance becomes an important parameter to track. Your organization's employees may be compliant with all your information security policies, but that is not enough when you are dealing with third-party vendors who have access to your organization's data.

Tracking compliance is a major issue that arises when dealing with third-party vendors. As discussed before, it is difficult to control the way in which third-parties operate. Therefore, whether or not they are compliant with the security policies in your organization or those defined by regulatory bodies and industry standards will be difficult to track. If they are not compliant, you may be putting your customers' data in grave danger by sharing it with the vendors.

Authorization of access to data

A major problem that arises due to the lack of visibility into the operations of third-party vendors is that organizations may not know who has accessed the customer data shared with them. It becomes difficult to keep an eye on how the employees hired by your third-party vendors are handling the data that you collected from your trusting customers. If unauthorized or untrustworthy personnel members are able to access your sensitive data, it can jeopardize your business operations in a big way.

Encryption of data

Many kinds of data require encryption as an additional layer of protection against cybercriminals. With third-party vendors, you may not know if your data is being shared with the authorized staff using adequate encryption. This problem could be even bigger if the terms of your contract with the third-party vendor do not dictate how any company data must be secured before sharing it with other staff members.

Reputation among customers and peers

Your customers trusted your organization with the protection of their data when they decided to purchase a product or service from you. As the savior of their data, your organization will be the first one to be blamed when a security breach happens, even if it is due to a third-party vendor. Thus, when you hire a third-party vendor to help with any part of your business operations, you are risking your organization's reputation among your customers as well as your peers.

Financial stability

Loss or leakage of sensitive data through your third-party vendors can affect the financial stability of your organization. This is especially of concern when the data being shared with your vendors is financial information such as credit card details, tax information, insurance data, or details pertaining to any form of online payment. Dwindling financial stability could be an after-effect of reputational risks, regulatory notices, and loss of customer base. Therefore, this is a high-impact risk posed by third-party vendors.

Difference of physical location of third-party vendors

Another problem arises when your vendors are located in a different country than your organization. Further, the problem can escalate quickly if there are multiple third-party vendors located in multiple locations spread globally. There are several issues associated with this difference of physical location of third-party vendors:

(1) Information security regulations differ from one country to the other. Therefore, laws that dictate data encryption and set limits on what kind of citizen information can be transmitted across continents will vary. Your organization's security team will thus have to accurately understand each and every regulation that affects the handling of your data assets. Similarly, the vendors must also be aware of what laws they need to follow as the data provided to them will be for citizens from another country.
(2) As the laws governing data assets would differ from one country to the other, it could be difficult for your team to check if your third-party vendors are compliant with the set rules. This could be due to the physical distance, or incomplete understanding of the regulatory requirements.
(3) It is also possible that you hire different third-party vendors to do the same task in different countries. This is more likely when your organization conducts its business operations through multiple different geographical locations. This will make it difficult to streamline the vendor operations and set common vendor assessment criteria.
(4) Communication with third-party vendors is an issue, too. If they are operating from a different country, the communication gap will widen even further. There could be linguistic barriers that could limit the understanding of how your third-party vendors handle your organization's data assets. There could even be large time zone variations that can hamper all business-related communication between your information security team and the third-party vendor.

The risks mentioned in this section are only some of the many risks that could arise from a third-party vendor. It is important for all organizations to be vigilant and prudent when hiring a vendor for help with any part of their business operations. Now that we know what kind of risks can be posed by a third-party vendor, it is time for us to start thinking about how to manage these vendor risks and secure our data assets.

Vendor Risk Assessment

We have now understood the variety of risks that third-party vendors can pose to your organization and its business operations. To manage these risks, risk assessment is the first step to be taken. Let us take a look at how you can assess the vendor risks in your organization.

Prepare a list of all third-party vendors

The first thing you need to do is to prepare a list of all the vendors working for your organization, irrespective of their capacity. This database should be accompanied by a detailed description of how each vendor uses the data shared with them by your organization. This will include the way they process your data, store it, and share it with employees within their organization. It will also include which employees in the vendor's organization have access to the shared data. Further, it is important that you understand the impact that each risk can have on your data assets. We will discuss this more in the next step.

Classify the vendors depending on the risks they pose

From the first step, you would know what vendors work for you and how they endanger your data assets. Based on this information, you need to categorize each vendor into different risk levels – 'no risk,' 'low risk,' 'medium risk,' or 'high risk.' You can also construct your own risk categories depending on the nature of the data assets shared with a third-party vendor, the time for which it is shared, the nature of the risks the vendor poses, etc. No matter how you end up classifying the vendors, the method and criteria must make sense to you and should be universal.

Gather regulatory updates on your vendors

If your third-party vendors are governed by the laws and rules of regulatory bodies from the government or the industry, find out if they are compliant with those regulations. This will be an important part of vendor risk assessment, as it will inform you of how trustworthy and careful your third-party vendors are. Impressive compliance records will also help you gain confidence over your choice of vendors.

Design a remediation policy

A vendor risk assessment must lead to the development of an effective remediation policy that is able to eliminate all the risks identified in the first step. Link each risk with a corresponding remediation method so it is easier for your organization to follow when a risk becomes live. This will also help integrate risks with remediation, a step in the vendor risk management plan that we will talk about in greater detail towards the end of this book.

Since risk assessment is the first step in any risk management workflow, it is crucial that this evaluation be conducted flawlessly. Any mistakes here can prove to be disastrous for the steps that follow. Perform a thorough vendor risk assessment for managing your vendor risks smoothly. In the next section, let us look at some of the ways in which can prevent the risks that we described in the previous section from threatening your organization.

Preventing Vendor Risks

Once you have finished assessing the vendor risks in your organization following the steps we described in the previous section, it is important to think of the ways in which you can prevent these risks from penetrating your information security framework. If the risks are unable to breach even your most vulnerable data assets, security will be guaranteed.

Here are some ways of preventing vendor risks from breaching your organization's security barrier.

Setting vendor standards is important

It is important to set well-defined standards for all third-party vendors that work with you. The standards could be common for all vendors, or they may be customized to each individual vendor depending on the kind of data that is shared with them. They should cover all criteria from the vendors' compliance records to their standing in the industry and customer feedback.

Rate your vendors and enforce accountability

Once standards are set and communicated to your vendors, it becomes easy to demand accountability for information security. This also gives you a scale to rate your third-party vendors and decide if a new vendor is appropriate and safe for your organization. It is important that you judge every single one of your third-party vendors according to the criteria set in the previous step. Before you hire a vendor, make sure that they check all the boxes on your list of standards. Also, make use of the vendor risk assessment that you performed before to see if the vendor is well-suited for your operational needs.

Ensure that your vendors also have a risk remediation plan

We have already mentioned before that vendor risk management is a collaboration between your organization and your third-party vendors. It is not enough for your organization to have a rock-solid risk remediation plan. You must ensure that your vendors also have a thorough risk remediation policy in place. This is important because if a risk originates from your vendor and they are the first ones to identify it, they should also be the first to control and contain the risk. This would be impossible without a detailed remediation policy. When you hire a new third-party vendor for your organization, ask them for their own remediation policy so you can also alter your organization's vendor risk remediation plan accordingly.

Track vendor activities that pertain your data assets

We have already mentioned that the lack of visibility into vendor operations is a major risk factor with third-party vendors. One way to get around this issue is to constantly monitor any actions that your vendors take with your data assets – sharing, processing, storing, etc. You can also recommend any changes necessary to best safeguard your data assets. The permission to monitor your data-related operations should be a part of your agreement with the third-party vendor.

Monitor vendor risk remediation efforts

Since vendor risk remediation is a collaborative task, it is important that your information security team keeps an eye on the remediation efforts being taken by any vendor that posed a live threat to your organization's data assets. If their measures are not up to the mark, your team should recommend changes to the policy through a healthy discussion of the consequences of different vendor risks.

Periodic vendor assessments

No matter how long you have been associated with a third-party vendor, you must conduct regular vendor assessments. Their performance must be regularly monitored and judged based on a list of key performance indicators (KPIs) that your security team should develop. Periodic vendor assessments will prevent your vendors from slacking in their side of the job. It will keep them compliant with your information security policies as well as the regulations set by the government or the industry. Moreover, it will help you identify the high-risk vendors early on, so you can think of hiring a replacement.

Managing vendor risks involves a lot of risk prevention. However, preventative measures may not be sufficient at times. This is where risk remediation comes into play. In the upcoming section, we have described the various ways in which you can remediate the vendor risks that somehow manage to overcome the security controls installed by you.

Vendor Risk Remediation

Despite taking thorough measures to perform a vendor risk assessment and prevent the risks from becoming dangerous, it often happens that malicious actors find a way to penetrate the security barriers in organizations. It is for such situations that organizations must prepare risk remediation plans. Vendor risk remediation is a contingency plan prepared to thwart any incoming vendor-associated risks. It is also an operation that requires extensive collaboration from your third-party vendors too.

Let us take a look at the various steps one must take in order to remediate vendor risks in an organization.

Design a remediation plan

The first step one must take is to design a fool-proof vendor risk remediation plan for the entire organization. Since each vendor may pose a different set of risks, it is important that distinct remediation plans be prepared for each third-party that works with you. The plan should be based on the vendor risk assessment that we discussed earlier.

As we have already mentioned at the beginning of this section, vendor risk remediation planning must also involve the concerned vendors. Risk assessment informs you about the kind of vendor risks that your data is facing, the impact the risks may have on your data assets and business operations, and the risk weight or priority-level associated with each vendor.

Your remediation plan must take into account the factors mentioned above. Prioritization of vendors is particularly important when a risk that is common to multiple vendors working with you becomes live in your organization. In such a situation, it helps you choose which vendors need to be addressed first. This will save you time and make the remediation process a lot more efficient.

Communicate with your vendors

Communication is a key step in any remediation workflow. It holds even more importance when it comes to vendor risk remediation because communication with third parties is not as simple as communicating with team members or employees within your organization. Therefore, when a vendor risk penetrates your information security barrier and affects your data assets, you must act promptly and communicate the following information to your third-party vendors: (1) what data assets were compromised; (2) any updates on the cause or source of the compromise; (3) what risks may accompany the current threat; (4) what you need the vendors to do at their end; and any other information that is relevant to a given vendor. With this information, the vendors are likely to recommend specific remediation measures that might work depending on the vulnerability of data assets and the impact of the risks in question.

Communicate with your customers

Communication is not limited to third-party vendors alone. You must also share vital information with other stakeholders as well. Customers, for instance, must be made aware of the extent to which their private data has been compromised. They should also be assured of preventative action by sharing with them the kind of mitigation measures your organization is undertaking to prevent

further damages. Sometimes, a risk may even necessitate some preventive action at the end of the customer. In these situations, you should put together an easy-to-understand and easy-to-follow plan for your customers, while explaining to them the importance and urgency of taking these preventive actions.

Communicate with regulatory bodies

In some cases, regulatory bodies, whether they are government-based or from the industry, should also be informed about the risks and the damages caused to the data assets. This is especially important if you are made aware of non-compliance with regulatory policies by your third-party vendors. This is also because eventually, your own organization will also be audited for its compliance with regulations. When that happens, it is best to let the authorities know how aware and concerned you are about the safety of the sensitive and confidential data procured from your customers and employees. This will help you ensure business continuity in the long run.

Communicate with your own information security team

Do not forget to keep your entire information security team in the loop about all the risk and remediation related responses from your vendors. It is also important to establish a proper communication channel between your team and your vendors' teams. They should be able to connect with each other on a regular basis. This will improve the collaboration between your information security team and the corresponding teams from your third-party vendors. They can feed off each other's ideas to improve the overall security of your data transactions. This will be very beneficial for improving the visibility of data handling by your third-party vendors.

Bring in a third-party mediator

Hiring a third-party vendor to resolve a risk associated with another third-party vendor may seem counter-intuitive at first. However, it might be the most feasible option at hand when your third-party vendors are difficult to work with and have a history of non-compliance with information security policies. The third-party mediator can help smoothen difficult conversations with vendors, such as holding them responsible for endangering your data assets. It will also help prevent organization heads from blaming each other for inefficient risk prevention measures. In the end, third-party mediators will prove to be unbiased and impartial and help quicken the vendor risk remediation process.

Make all vendors accountable

When it comes to an information security risk that may threaten the business operations of your organization, you must make sure that anyone and everyone responsible for propagating the risks, performing assessment and undertaking remediation are held accountable. This is even more important when the risks are posed by third-party vendors. All vendors must be treated in an unbiased manner and held accountable for any mistakes at their end. An important way to improve accountability is honest, direct, and transparent communication with the vendors about your expectations and requirements.

Keep some back-up vendor options in mind

When push comes to shove, you should not hesitate to cut ties with a vendor that has endangered the security posture, reputation, and financial stability of your organization. This is an important remediation step that requires thorough pre-planning. You must create a list of alternate vendors for each product or service you obtain from your current third-party vendors. These alternatives must also be checked and approved for their compliance records and should match the standards set by your organization. This way, in case you need to let go of a previous vendor, you will have a new one ready. This will minimize the losses to your organization's business operations.

The steps described above must be followed to ensure adequate remediation of vendor risks in your organization. In the next section, we discuss how vendor risk remediation can be made even more effective by integrating risks and remediation.

Integrating Vendor Risks with Remediation

In the previous section, we saw the steps required to be taken to ensure an effective vendor risk remediation strategy. These remediation measures can be made better and prompter by integrating them with vendor risks at the start of the vendor risk management program. Let us see how one can achieve the integration of vendor risks and remediation.

Collaboration with third-party vendors

Collaboration has been a recurrent theme throughout this book because it is just that important when it comes to managing vendor risks. Inputs from the vendors as well as your organization's own information security team when performing risk assessment and designing vendor risk remediation policies can help make the process a lot more efficient. Collaboration improves the transparency of business operations and the overall information security workflow. This cooperative process will directly link each identified vendor risk to a corresponding set of remediation measures, thus organically integrating risks and remediation.

Vendor risk reassessment

Any risk remediation step must always be followed by a reassessment. Reassessment allows you to see if the steps you took to contain or eliminate the risk worked. It also helps you evaluate the vulnerabilities of your data assets again. If you identify that your remediation steps were not enough to contain or eliminate the vendor risk in question, you also have the opportunity to design a new policy that can help minimize the impact of the risk now. Since reassessment inherently involves comparing risks and their remediation steps with current data vulnerabilities, it automatically integrates vendor risks and remediation with each other.

Integration starts with vendor risk assessment

Vendor risk assessment, as we have discussed before, is the first step in vendor risk management. If you start linking remediation measures with each identified vendor risk at the stage of vendor risk assessment itself, integration of risks and remediation will become much simpler. This is particularly useful if your organization has hired several vendors. The vendors will also be classified into risk categories beforehand during risk assessment, which will make the assignment of remediation measures easier.

Monitor the remediation measures being taken by your vendors

When a third-party vendor risk becomes live, you not only have to keep a track of the remediation measures being taken in your organization but also of the steps being taken by your vendors. This will help you update your remediation policies based on the efficacy of the steps taken by your vendor. In addition, it will require you to verify that each risk has a corresponding remediation measure underway either in your own organization or in your vendor's. This process closely integrates vendor risks with remediation and helps make the risk management workflow efficient.

Apart from the methods mentioned above, there is another way in which vendor risks can be integrated with remediation – automation of the vendor risk management process. It does away

with the excessive time and financial and human resources needed for vendor risk management and helps make the entire security operation very robust. The next section is dedicated to the benefits of automation when using BizzSecure’s EAID solution.

Automation of Vendor Risk Management with the EAID Solution

As the entire world is becoming more and more digital every day, all aspects of life are also slowly graduating to automation. This is also the case with information security and risk management, which when performed manually can be very tedious and error prone. Automated portals provide an effective way of streamlining the different steps in an information security workflow. They promote the judicious use of resources, both financial and human. Moreover, they greatly improve the visibility of risks and the corresponding remediation operations.

BizzSecure presents an all-in-one automated platform to meet all your security risk management requirements – the Enterprise Assessment and InfoSec Design (EAID) solution. This platform can be accessed as a monthly subscription to make your organization's risk management simple and robust. Here are some of the advantages of the EAID solution in the context of vendor risk management.

Managing multiple vendors simultaneously

Automation through BizzSecure's EAID solution helps in the proper management of multiple vendors working with your organization. Automation achieves this using the simple yet effective medium: questionnaires. Questionnaires serve as a way of collecting user input about the state of an organization's security posture. They can be designed to be filled out by all the stakeholders in an organization. Questions can focus on specific security topics related to vendor risks and compliance.

Tracking compliance

The EAID solution comes with several in-built regulatory policies that when selected can help you understand what criteria must be monitored to be compliant with regulatory authorities such as federal or state governments and the industry. Depending on the kind of data you are sharing with your third-party vendors and the regulations that govern the operations of the vendors themselves, you can choose one or more policies and keep track of compliance through the questionnaires mentioned above.

Improved credibility of vendors

This is an engaging way to include your own employees as well as those from your third-party vendors into the risk analysis and remediation process. The questionnaires do not simply seek answers, but also demand evidence to corroborate them. This increases the credibility of the method. Further, since the questionnaires can be kept common for all vendors, it gives your organization a unified platform to evaluate them at the same level.

Enhanced visibility into the operations of third-party vendors

With the help of questionnaires, an automated platform also gives your organization insight into the functioning and compliance levels of your third-party vendors. This does away with the previously discussed problem of lack of visibility of vendor organizations.

Better communication with vendors

Another area where automation really helps is communication. We have discussed in detail the importance of quick and honest communication in any information security operation. Automation allows an organization to authorize multiple users who can access a given questionnaire, which includes members from third-party vendors. Moreover, it allows you to compile progress reports about risk remediation and mitigation which can be easily and quickly shared with the concerned third-party vendors.

Real-time assessment and remediation of vendor risks

In the automated EAID solution platform, you can visualize all your third-party vendors on a single screen simultaneously. They are all easily integrated into the automated portal which allows you to look at the risks associated with each vendor and remediation measures, if any, that are ongoing at a given time. Any updates to the security posture based on third-party vendor risks can be easily tracked in real-time, which makes the security framework highly effective.

Maturity of vendor risk management

The EAID platform allows you to compare your remediation measures and risk assessment reports from a previous year to the current reports and understands how your security framework and vendor risk management efforts have matured over time. This is important if you want to develop better vendor risk management policies in the future. You can also send these reports and analyses to the concerned third-party vendors so that they too can improve their respective information security policies based on past experience.

Integration of vendor risks and remediation

In the previous section, we have already discussed the various ways in which vendor risks can be integrated with remediation measures. Automation is another way in which the integration of risks and remediation can be achieved in an organization. The EAID solution immediately makes both vendor risks and their associated remediation measures visible to the organization. It allows you to assign specific mitigation steps to each risk, which inherently links risks with remediation.

Automation of vendor risk management through BizzSecure’s EAID solution has a lot of benefits that can change the landscape of information security in your organization. Subscribe to the EAID solution to avail of these benefits today.

Conclusion

Vendors pose some of the greatest threats to information security in any organization. Managing vendor risks is therefore crucial to the success of any information security workflow. Like any risk management program, vendor risk management also requires three fundamental steps: risk assessment, risk prevention, and risk remediation. Through this book, we have attempted to touch upon each of these steps in the context of vendor risk management.

We first discussed the different ways in which vendors may expose your organization to cybersecurity threats. We followed this with the steps one must take to conduct a vendor risk assessment and the ways in which you can prevent these risks in your organization. The next section elucidated the ways in which vendors' risks can be remediated should they become live. The last part of the book dealt with how automation of the security workflow using BizzSecure's EAID solution as the platform can immensely help to manage vendor risks efficiently and quickly.

The EAID solution encompasses all the steps in vendor risk management and integrates on a single platform. Therefore, no matter what scale of business operations you run or how many third-party vendors you have working with you, follow the steps we have described in this book and think of the EAID solution when updating your vendor security management program.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com