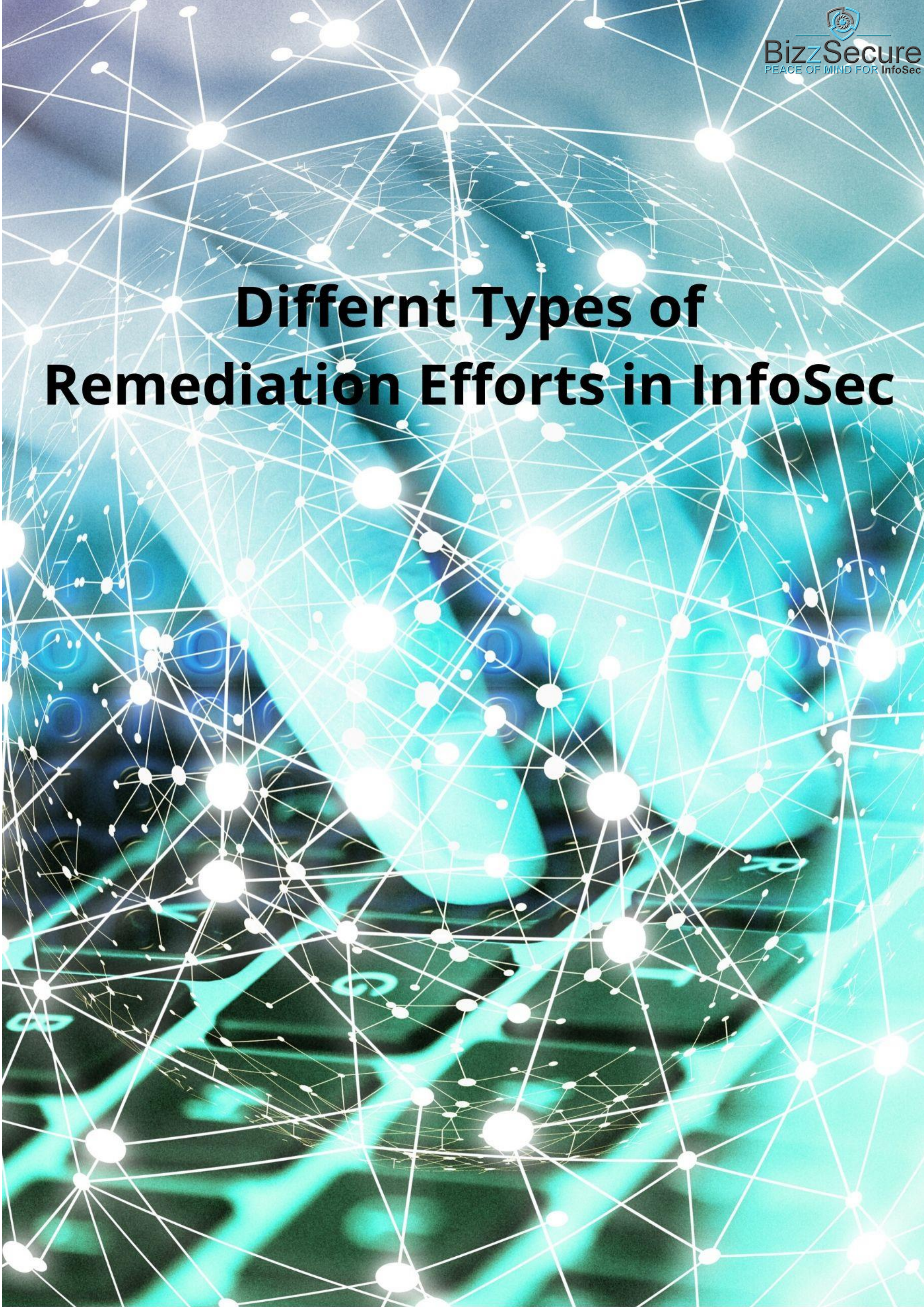
BizzSecure
PEACE OF MIND FOR InfoSec



Differnt Types of Remediation Efforts in InfoSec

Table of Contents

Introduction

The number of ways in which an organization's confidential and private data can be mishandled, leaked, lost, or misused by people with malicious intent is growing by the hour. As digital technology excels in data handling, so do the risks associated with it. To make matters worse, digital information is not the only kind of data at risk. Physical hardcopies of sensitive data could also be endangered by unauthorized personnel and thieves. Additionally, apart from external factors, there are also internal factors that could contribute to reduced information security in an organization – non-compliance.Non-compliance with the information security and regulatory policies that have specifically been designed to protect your organization can prove to be the most dangerous of all the risks to information security. In the end, all of these risks work together to disrupt the business continuity of organizations.

Thus, your organization's data assets are faced with risks related to network security, application security, container security, physical security, third-party vendor security, compliance, and business continuity.

Risk remediation is the key to ensuring that all these risks that may be endangering your organization are contained or eliminated appropriately. Since there are so many types of risks to information security in any organization, there are also multiple kinds of remediation efforts to counter such risks.

The purpose of this book is to get you acquainted with the different types of remediation efforts in InfoSec so you can protect your organization against any number of information security risks. We start with the remediation efforts required to manage network security risks and move on to remediating risks related to application security, container security, physical security, third-party vendor security, compliance, and business continuity, in that order. Let's get started.

Remediation of Network Security Risks

Network security risks are some of the most common information security risks in this world that is run by the internet. All e-commerce and long-distance financial transactions are highly dependent on network connectivity and how secure the connection is. This is perhaps one of the most vulnerable aspects of digital information. Hackers regularly target poorly secured networks to extract valuable information for malicious purposes.

It is, therefore, extremely important to secure your all networks over which your organization's data is transmitted – internal or public. If the networks are not secure enough, or if the hackers find a way to breach the security barriers that you have installed, the only countermeasure at your disposal would be your network risk remediation policy. Let us look at how you can remediate the network security risks endangering your organization.

Phishing emails

Phishing emails pose one of the most serious threats to your organization's digital information. Hackers regularly target companies by sending out emails pretending to be an official entity, the government, or some other email sender that employees would easily assume to be important. If your employees are not careful, they couldopen these emails, and perhaps even click on the malicious links shared through them. These links could direct them to forms or other web pages that require them to feed information such as their credentials or other private and sensitive data. This always ends in the data being stolen for misuse. The best way to remediate the risks posed by phishing emails is to (1) request your employees to flag such emails as 'phishing' and immediately inform the information security manager at your organization, and (2) inform all your employees and even customers (if required) about the onslaught of phishing emails and ask them to be vigilant and cautious when opening any such emails and the attachments shared through them.

Unsecure networks

Another important area to address when remediating network security risks is sharing company data over unsecured networks. This could be when your employees are working remotely from their homes, a café, or some other location that is not as secure as your company's network. If you discover a network breach by your information security team or other employees, you must ensure that every other piece of crucial data in your organization is encrypted using algorithms or software that are secured appropriately. Also, once again, all employees must be informed of any network security breach and warned of the perils of sharing their data on an unknown network.

Change your passwords

If and when a network gets breached, you must immediately think of who had access to the network and the files shared on it. If the network password is suspected to be compromised, you must immediately change it. Make sure that your employees do the same for their business computer network passwords as well. Moreover, guidelines on creating secure passwords must be circulated among all employees at such a time so that they are reminded of how passwords can be made more secure. These guidelines could include points such as (1) use passphrases instead of passwords as they are much more difficult to guess, given the spaces and punctuation involved, and (2) the best option is to use multi-factor authentication systems that rely on multiple inputs of different forms such as a passcode sent on a mobile phone or a phone call, etc. from anyone trying to access a system, network or file.

These and many other steps could be taken to ensure that network security risks get remediated in your organization. Next, we look at application security risks and how to remediate them.

Remediation of Application Security Risks

Applications are running today’s world of digital information, on laptops, mobile devices, and tablets. Applications could be developed in-house by an organization or purchased from third-party vendors. These little chunks of software have truly changed the way the world works today. Unfortunately, they have also prompted malicious actors to come up with new ways to harm organizations’ data assets.

Modify the way application access is granted to your users

Gaining unauthorized access to an organization’s application data is becoming an important way in which sensitive data is getting compromised. To remediate such risks, it is important to re-evaluate the way access is granted to the application users in your organization. Check if you need to change the access to some applications that handle sensitive data. You may want to take away access from some non-essential personnel members. You could also think of changing the way access is authenticated. Choose a multi-factor login system to add an extra set of security measures when granting access to an application.

Alter the source code for applications built in-house

All application programs have unique blocks of codes that some hackers find easy to target. In case an application security risk becomes live, your information security and application development teams should work together to identify these unique codes and alter them to make the applications less vulnerable to such attacks.This step can even be taken up early when the application is in its test or launch stage. An assessment of application vulnerability at this stage would prompt developers to add more protection to the application before it is released for use in your organization.

Ensure that all employees and third-party vendors are compliant

We are going to talk about compliance in detail in its section later, however, this becomes a crucial issue when thinking of application security. This is because most of the applications used to handle data in an organization are purchased from third-party vendors that, as we will see in a later section, could make your customers’ data highly prone to information security risks.

As we have mentioned before, non-compliance is the prime enemy of any information security measure. This is also true for application security policies which, if not adhered to, can put all your application-based data transactions at great risk.

All application security policies, irrespective of whether the applications were developed within your organization or purchased from a third-party vendor, demand compliance from both your employees and any involved third-party vendors.

Security policy could dictate a variety of protective measures such as captcha-based login, passphrases instead of passwords to login into an application, encryption of all data being shared on an application, encryption of the application itself, etc. The third-party vendors developing such applications must abide by regulatory laws and policies set by the government and the industry.

Look for updates to the applications used in your organization

Application technology keeps evolving every day, just like threats to information security keep getting upgraded. When remediating application security risks, it is necessary to think of changes happening in the cybersphere that could make hackers stronger as well as those that could make your applications stronger. Application developers are constantly releasing newer versions of their applications to improve on function, features as well as security. This is true for the applications built in-house as well as those purchased from external sources. Think of what kind of updates in technology are available that could make a compromised application less vulnerable to data loss and leakage. The IT, InfoSec, and third-party vendor teams must work together to make the applications safer at the level of the application code itself. In some cases, you may even have to decide whether a new third-party vendor is more reliable, secure, and compliant than your current application vendor. All these measures will help remediate some of the most important application security risks in your organization.

Manage container security risks

We have dedicated the next section to container technology and how it has become a hotspot for new targeted attacks on information technology and organization data. Containers are used to store different applications in the same location, but still in isolation from each other. The technology is supposed to make applications more secure, which is exactly why so many hackers are now targeting it. Overall, container risk assessment and remediation is an important part of application security risk remediation itself. As part of application security risk remediation, your information security and IT teams must look at the host operating system being used to run the applications stored in containers. If required, the host operating systems must be modified. It is also necessary to see if the container images or raw files were made in-house or purchased from a vendor. In either case, the vulnerability of the images must be determined. For containers built in your organization, you could even consider changing the images and getting new ones from a more reliable source. We will discuss this further in the next section.

Use the steps described in this section to remediate all application security-related risks in your organization. Read through the next section and incorporate container security in your application security risk remediation strategy as well.

Remediation of Container Security Risks

We have already discussed one of the most defining developments of recent times – applications. We also briefly introduced container technology in the previous section. The world of applications has not too long ago developed a new partner in the form of container technology. Containers, much like shipping containers, are locations (only virtual in case of the digital world) where multiple applications can be developed, stored, secured, accessed, and operated. Container technology was supposed to keep the applications secure too, but hackers have started seeing containers as potential targets to gain access to your application data. Therefore, it is important to know what kind of risks containers pose and how to remediate those risks, should they become live. Let us take a look.

Containers developed in-house

Containers could be developed by your organization if your employees, or IT department, in particular, have the required expertise and know-how. Other times, containers are simply purchased from third-party vendors. For containers developed in-house, any event, in which a container security risk becomes live, must trigger the following remediation actions: (1) the IT and InfoSec teams must check the sources of the container images used because these parts tend to be the most vulnerable, (2)the host operating system must be checked to see if it has been compromised in any way, and (3) individual applications stored inside the compromised containers must be assessed to know the impact of the identified container security risk on their function and stored data.

Containers purchased from third-party vendors

If your organization uses containers purchased from third-party vendors, you must follow the remediation measures that we have already discussed for the remediation of third-party vendor risks. Aspects of application security risk remediation measures must also be integrated with container security risk remediation.

Do not be afraid of implementing the relatively new container technology in your organization. Even though there are risks associated with them, containers are fundamentally designed to protect the applications they store. Always be prepared to implement the container risk remediation steps to protect your data assets in case of a security breach through the containers. Next, let us look at remediation from a more holistic and a big picture perspective – remediation of business continuity risks.

Remediation of Physical Security Risks

Information security risks are not limited to the digital world, even though most of the information today is, in fact, digital. Physical factors are equally as risky to your organization’s data assets. You may wonder: how is that possible? Information in both digital and paper-based formats can be endangered by physical security risks.

In the digital format, the devices that store your organization’s data, such as hard drives, flash drives, etc. can be under risk of physical damage caused by a natural or man-made disaster, electrical fires, thefts, and other such physical factors.

Paper-based information, such as print-outs, hardbound copies of documents, photocopies, fax, etc. containing vital information about the business operations of the organization, can also get damaged in similar ways due to disasters, fires, or thefts. Additionally, they could simply be read by someone who is not authorized to access the information. This poses an extra risk.

Increase the security of your physical data storage devices

The first thing to do when it comes to remediating physical security risks is increasing the physical security of all the devices that store your organization’s data assets. This means (1) check who is authorized to access the physical locations where your organization’s printers, computers, servers, external hard drives, flash drives, etc. are kept, (2) if they are not already, put all easily portable devices under lock and key, (3) physically segregate critical equipment that is housing your organization’s data by putting them in separate locked rooms, and (4) ensure that your CCTV cameras are functional and check the footage to identify troublemakers in the event your premises have been broken into and robbed.

Communicate with government authorities

In the event your organization’s physical security has been threatened by a natural disaster such as a hurricane or a flood, you need to be on the constant lookout for government advisories on how to handle the situation. Follow regulatory guidelines for regular updates to the intensity of these disasters, how vulnerable your organization’s premises are to them and evacuation strategies.

Immediate back-ups

If any of your company data that is vital to business operations has not been backed up, the InfoSec and IT departments must collaborate to ensure that back-up files are prepared immediately when a threat is imminent. Back-ups should be secured both digitally and physically so that current and foreseeable future risks cannot damage them.

Shredding of documents with critical information

Paper-based documents must contain the organization’s critical data and must be disposed of in ways that are pre-approved by the management. This could involve shredding or incinerating the documents. Destruction of printed or copied information must be done immediately after the information has been used or when you gain knowledge of a risk becoming live in your organization.

Physical security risks could be some of the most unpredictable risks in any organization. As such, remediation measures need to be strong and robust. Include the steps mentioned in this section in your organization’s physical security risk remediation policy for an effective security management framework. In the upcoming section, we look at how to remediate third-party vendor risks in an organization.

Remediation of Third-Party Vendor Risks

Third-party vendors pose the highest and the most potent risks of any vulnerable components of your business. The reason is that these vendors work independently most of the time, so you have no visibility of what is going on in their organization. Even if organizations collaborate with them, they often find it difficult to judge if the third-party vendors are prudent and vigilant enough while handling data.

Let us take a look at how you can remediate the third-party vendor risks in your organization.

Develop a remediation plan in collaboration with your vendors

Developing a remediation policy is an important first step for any kind of remediation, but it becomes even more important in case of third-party vendor risks. Addressing such risks requires a collaborative effort from both your organization and the third-party vendor(s) involved. Multiple customized remediation plans should be formulated based on the data shared, vulnerability, and risk associated with each third-party vendor.The third-party vendors should be able to provide suggestions on how to remediate a risk that has become live. They should also incorporate suggestions from your organization's information security team into their remediation plansespecially when handling the data obtained from your customers. It is also important to prioritize vendors when you are working with several different third-parties. Evaluate the kind of impact the risks associated with each vendor would have and assign a weight or rank accordingly. When a risk becomes active as a result of two or more vendors, act according to the priorities assigned. This will increase the efficacy of your information security workflow.

Communication is important

We have previously highlighted the importance of communication in other sections and will focus on it again later. Communication with your third-party vendors when dealing with vendor-related risks is very important. They must know what portions of the data they are handling for your company are vulnerable or have already been compromised. Details of what your remediation policy entails must also be communicated promptly so that they can suggest changes if required like we discussed in the previous step. Constant communication with third-parties based in countries different than your current location can be difficult but must be had nevertheless when a risk becomes live. It will also help if you could share any risk assessment reports created by your information security team with the third-party vendors involved. This way, they will know what they have to be prepared for in terms of the scale and efficiency of remediation efforts.

Make vendors accountable

It is very important to make all third-party vendors accountable as part of risk remediation efforts. Work with all the third-party vendors in an unbiased manner and ensure that they take remediation of risks very seriously. Keep tracking the progress of the remediation efforts undertaken by the third-party vendors. Also, seek regular reports on the efficiency of their security operations.

Involve an impartial third-party to mediate

Communication and collaboration between organizations and their third-party vendors is not always perfect for several reasons. Lack of proper communication could lead to poor remediation measures for third-party vendor risks. Another problem is that people often fight over who should take the blame for exposing an organization’s data to risks. Is the organization responsible? Or should the third-party vendor take the blame? To avoid such situations, it is important to involve a third-party mediator who is impartial to both parties. They can help set up an effective communication channel and oversee the security operations on both sides of the situation. The hired third-party could also be a security expert who can then provide their inputs on how to remediate the existing third-party vendor risks in your organization.

Given the high risks posed by third-party vendors, fool-proof remediation plans must be formulated to deal with situations when a third-party risk becomes live. Follow our steps and prepare your organization. In the next section, we will discuss how compliance-related risks also need to be remediated to maintain the security posture of an organization.

Remediation of Compliance Risks

As we have mentioned before, non-compliance with internal and regulatory information security policy is perhaps the biggest information security blunder an organization could make. It greatly compromises the risk management system you have in place. Therefore, your employees who are not being compliant with the various policies that pertain to information security are in fact propagators of compliance risks in your organization. Let us look at how you can remediate compliance risks in your organization.

Train your employees

Lack of training and general awareness is the foremost reason for the existence of compliance risks in any organization. You must conduct regular training sessions for all your employees, no matter where they lie on the power pyramid. Even your top-tier executives and board members must go through such training sessions. This will inculcate the importance of compliance in the entire workforce of your organization.

Monitor user activities

If a complaint of non-compliance has been made against a given employee, you may have to track the ways in which that employee is using your data and digital resources to understand if stringent action must be taken against them. You may have to change the access control associated with such employees and the kind of data that is shared with them.

Self-audits

Internal audits of compliance in your organization could be a great measure to remediate compliance-related risks in advance. You can ask your employees to fill out a carefully designed questionnaire that questions them about their compliance habits. These questionnaires can also seek evidence in support of the answers being provided by the employees. Your information security team can then analyze the results of the audit and circulate the interpretation with all the stakeholders. Depending on how compliant or non-compliant your employees are at the end of the survey, you may have to update your remediation policies for the different kinds of risks discussed previously. This will also determine how frequent your self-audits must be.

Monitor changes in regulatory compliance requirements

If your organization is governed by one or more laws such as HIPAA or PCI-DSS, or industrial standards such as those set by ISO or NIST, you have to pay special attention to their respective regulatory policies. Non-compliance with such authorities can cause serious consequences legally as well as financially. To be able to remediate risks on time, keep track of the changes or updates in any of the regulatory policies that your organization is required to follow. Any change in these policies must also reflect in your organization's internal information security policies. Further, the changes must be communicated to all your employees so that they can stay compliant with them.

Eliminating compliance risks will solve half your problems. Next, we look at how to remediate risks to business continuity.

Remediation of Business Continuity Risks

The bigger picture in any information security framework is to ensure business continuity in the organization. No risk should be able to take a form that tampers with the future of your business operations. Therefore, ensuring business continuity is an important type of remediation efforts in information security.Here is what you can do to remediate business continuity risks in your organization.

Communicate with your security personneland other stakeholders

Business continuity is not specific to one department, like IT or InfoSec. It is a company-wide task and should be treated holistically. One of the most important requirements for this is a prompt and honest communication with all stakeholders in the organization. This includes your security teams (both InfoSec and physical), top-tier management, and third-party vendors if they are involved and even your customers.

Communication should be given enough attention to if your organization operates its business in multiple different locations and if several third-party vendors areworking for you. Depending on the specifics of the risk that your organization may be facing, all stakeholders must be communicated guidelines on how to handle the risk and any alternate remediation measures that could be effective in containing it. Business continuity risks emanating from third-party vendors must be discussed with them so their expertise can be timely incorporated with your organization's current information security policy.

Let your customers know about the ongoing situation so they can better prepare themselves for whatever may be about to come. Provide them information on how they can help mitigate the risk on their own. Last but not the least, assure them that you will help them out of the threat and that you are doing everything in your power to protect their sensitive data.

If your organization's data is protected by federal or state laws or other regulatory bodies, it is your duty to inform them of the risk and the kind of remediation efforts your organization is taking to eliminate the risk. We will discuss more about regulatory bodies in the forthcoming paragraphs.

Control who can access your organization's data

Unauthorized access to critical organization data is one of the most common ways in which information security threats propagate in an organization and disrupt business continuity. Therefore, to remediate business continuity risks, it is important that you step back and evaluate who among all your employees and third-parties has access to the information that is or could be vulnerable to a security risk. Certain situations may even require you to change the sensitivity classification of some of your information to regulate access more rigidly, perhaps on a 'need to know' basis. You may also have to re-evaluate your organization's password policy. we have already discussed this to some extent under the section on remediation of network security risks.

If in your evaluation you find that some people who should not have had access to sensitiveinformation were able to access it due to some technical or personnel faults, their access should be changed immediately. They should be questioned internally to know who they may have shared any sensitive information with, whether the receiving party is within or outside the organization.

Track your organization's risks and remediation in real-time

Part of remediating business continuity risks is to be able to track the effectiveness of ongoing efforts to contain or eliminate the root risks that are plaguing your organization, such as those related to network security, application security, compliance, physical security, etc. Your organization must also be prepared to deal with any potential new risks that could be coming its way. Tracking risks and remediation efforts in real-time gives you the ability to control the security operations closely and quickly, thus increasing the efficiency of the security workflow and ultimately ensuring that business continuity is restored.

Ensure compliance with regulatory authorities

Your business continuity is gravely threatened if your organization is required to abide by some federal or state laws and industry standards and then there is a data breach. In such cases, the regulatory authorities must be informed immediately of the kind of data breach, the data assets affected, the impact the risk is expected to have on the data assets and business in general and what your organization is currently doing to mend the security framework. If you do not inform the regulatory bodies in advance and are audited for security concerns, they could take legal action against your organization, depending on the scope of the regulation required to be followed.In the very least, they could black-list your company or ask you to suspend, reduce, or cease operations completely. This will, in turn, affect your customer base. Therefore, it is important to ensure that all your employees are compliant with the regulations put forth by the authorities.

Always stay up-to-datewith new developments in the cybersecurity world

As we design policies to thwart their incoming information security assaults, malicious workers seem to be evolving just as fast if not more. The problem is that sometimes, it is difficult to predict what the next risk is going to look like. Use pattern recognition systems and advanced technology to keep yourself up-to-date with information about the development of any new computer viruses or intrusion systems andnew technological advancements in hacking. If you can predict what an information security risk is going to look like in the near future, it will help us be more prepared for the remediation of such as risk when the time comes.

Business continuity risks are an amalgamation of all the other types of risks we have discussed in this book previously. If you follow all the steps that we have described in this book, you will automatically be remediating all business continuity risks in your organization.

Conclusion

Any organization that handles data at any level in today's world is a potential target of malicious hackers and intruders, trying to steal confidential data and misuse it for their gains. Such malicious actors have devised numerous ways to aim at different vulnerabilities in an organization. Naturally, there are numerous kinds of risks that an organization faces. To manage these risks efficiently, one needs equally as many varieties of remediation efforts.

Through this book, we hope to have explained to you the different types of remediation efforts in information security. The different kinds of risks and remediation efforts listed in this book will help you enhanceyour organization's existing information security policies and better protect the organization against the ever-evolving risks in the information security landscape.

When it comes to strengthening your information security policies, it does not matter if your organization is a new one or is already well-established in the field. We can all use a little help and improve our organizations' security. All the types of remediation efforts in InfoSec described in this book can be undertaken very easily through BizzSecure's Enterprise Assessment and InfoSec Design (EAID) solution, an automated all-in-one platform that streamlines the information security workflow in any organization. It helps you meet regulatory compliances, perform risk assessments, and track remediation efforts in your organization. To better implement the different types of InfoSec remediation efforts that we have discussed in this book, consider subscribing to BizzSecure's EAID solution today.

BizzSecure
PEACE OF MIND FOR InfoSec

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com