BizzSecure
PEACE OF MIND FOR InfoSec

How to Manage Business Continuity Risks

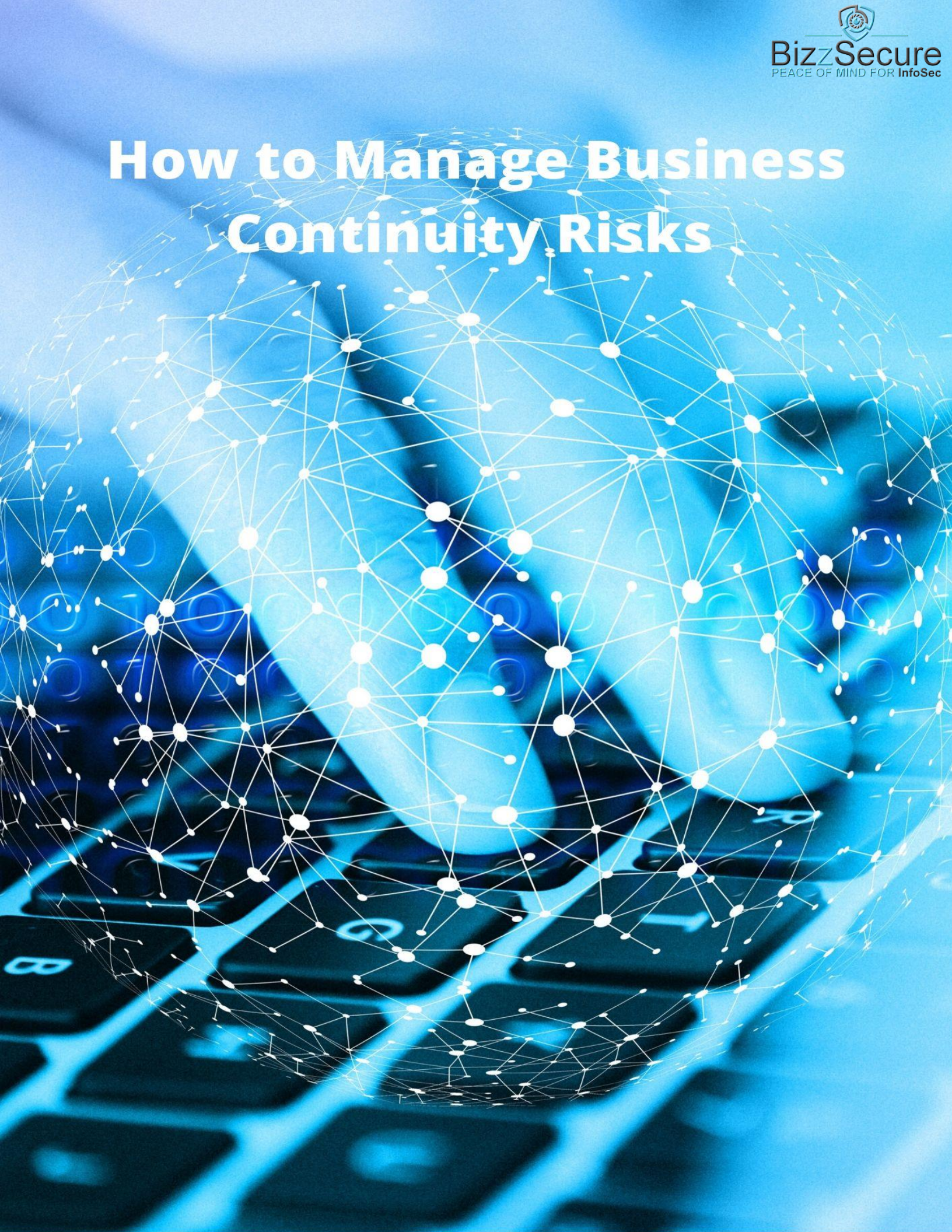

Table of Contents

Introduction

Put simply, business continuity refers to the sustainability of an organization's business in the event of a threat or disaster that impacts its assets. In the current age, these assets could be physical or digital. Since a large number of organizations today deal with some, or the other kind of data – be it from their customers or their employees – it has become important for them to ensure business continuity in case a data breach or leakage takes place. Indeed, even Fortune 500 companies have had to face the maliciousness of cyber attackers in recent times.

In the case of organizations whose business operations depend heavily on data handling, business continuity is an indicator of how secure their data assets are. Now, security encompasses a wide perimeter of assets and resources including network security, physical security, application security, container security, third-party vendors, and compliance. To ensure business continuity in any organization, it is important to analyze and manage all of the above-mentioned risk and security areas.

Management of business continuity risks is a highly important task that requires to major steps: (1) business continuity risk assessment and (2) business continuity risk remediation or mitigation. Risk assessment is the identification, analysis, and ranking of business continuity risks based on their nature, impact, and ability to be remediated. Risk remediation or mitigation is the set of steps an organization takes to eliminate or contain any business continuity risks.

In this book, we delve deep into the management of business continuity risks, highlighting the nuances of the two steps mentioned in the previous paragraph. We start with the different areas that are important determinants of business continuity in any data-based organization. We follow this with a discussion of the first step in business continuity management – risk assessment. We further elaborate on the steps one should take to ensure business continuity risk remediation. Lastly, we shed some light on BizzSecure's EAID solution, a holistic platform that aids you in the management of all the business continuity risks in your organization.

Business Continuity Risks in Organizations Involved in Data Handling

Prior to discussing the management of business continuity risks in an organization, it is important to understand the variety of areas that could be the center of business continuity risks. Here are the different classes and subclasses of business continuity risks that data-based organizations face regularly.

Network security risks

In the digital world that operates on the internet, network security is of the utmost importance. Networks, whether private or public, are the entry points for all hackers and intruders to gain access to your organization's data. If your data lacks encryption or password protection, it is going to be vulnerable to a large number of cyber risks. Therefore, it is extremely important to secure your organization's network.

Application security risks

Applications are the front-runners in all data handling operations in the present times. They help you run a lot of your business operations smoothly through laptops, mobile phones, and tablets alike. Needless to say, they have become prime targets of hackers engaged in unethical access and misuse of data. They have recently emerged as one of the biggest risk areas for business continuity.

Container security risks

Container technology represents a new era in application development, storage, and management. In a container, several applications can be stored and run together, while still being isolated from each other. Containers are meant to keep your applications more secure, but cybercriminals have not even left this technology unscathed. Therefore, containers also represent a major risk area that needs to be addressed to ensure business continuity.

Physical security risks

Data security is not limited to software and network security. Your data assets also need to be protected from physical damages or losses caused by natural disasters such as floods or hurricanes, man-made hazards such as fire, deliberate attempts at thefts in your premises, or inadvertent breakdown of your hardware or servers. A lot of these factors depend on the geographical location of your organization's premises. If you conduct business operations in more than one location, the risks tend to be even higher. Therefore, your business continuity faces a lot of physical security risks.

Third-party vendor risks

Your organization may have hired one or more third-party vendors who are responsible for providing specific software or hardware to facilitate your business operations. However, third-party vendors also pose the greatest risk to the information security and business continuity of any organization. This is because organizations do not have 100% visibility of the risks and remediation efforts in third-party vendor organizations.

Compliance risks

Even if you have planned to thwart any of the above-mentioned risks to your organization's business continuity, there is another important factor that can be harmful – your employees. We do not mean to say that your employees are bad for your organization. We simply mean that your employees have the power to completely change the efficacy of your security framework by deciding to follow or not follow the information security rules laid out in your security policies. Lack of compliance with security policies is a dangerous risk to an organization's security posture and business continuity.

In this section, we have covered some of the most important risk areas that endanger the business continuity of any organization that deals with data. It is now time to dive deep into the what and the how of business continuity risk management. The next section focuses on the steps you should follow to conduct a thorough business continuity risk assessment.

Business Continuity Risk Assessment

Now that we have looked at the kind of risks can harm an organization's business continuity, it is time to learn how to perform the first step of any business continuity management workflow. This step is an in-depth analysis of the specific risks that endanger the business continuity in a given organization.

Here are some important steps you must follow to perform a business continuity risk assessment in your organization:

Conduct an exhaustive risk identification

Risk identification is the foremost step in business continuity risk assessment. As the name suggests, this step requires you to identify any and all business continuity risks endangering your organization. Risk assessment should be exhaustive, including all the types of risks that we discussed in the previous section. Since risks vary rapidly with time and location, risk identification is also dependent on the time period and geographical location of conduction of risk assessment.

Evaluate all the physical locations in your organization

Depending on where your organization is located, it may be faced with different physical security risks to its data assets and storage devices. You must scan your organization in different geographical or physical locations to identify all the physical security risks that surround it. This will require you to know the kind of natural and man-made disasters your locations are prone to and the impact those disasters will have on your data assets.

Vendor risk analysis

If you have hired one or more third-party vendors to help with your organization's business operations, your data may be at more risks than you know. Your business continuity risk assessment must involve a thorough analysis of all the hired vendors, the kind of data they have access to, and how compliant their respective organizations are with your own security policies as well as the standards and regulations set by federal or state agencies and the industry.

Look at all the applications that your organization uses

Since application security risks form a major part of business continuity risks, it is important to take a deep look at the vulnerabilities of all the applications that your organization uses to conduct its business operations. Depending on the data these applications have access to and the vulnerability of each application, you can classify the applications into different risk categories for better remediation.

Container security risk assessment

As we discussed in the previous section, containers are designed to securely manage your applications. However, they still pose a major risk to your organization's business continuity. The container risk assessment will primarily include looking at the safety and trustworthiness of the

sources from which you obtain your container layers or images. It will also include assessing the safety of your host operating system kernel. If your organization is developing its own applications, you must conduct a container risk analysis separately. If your organization purchases applications from third-party vendors, container security risks can be evaluated under vendor risk assessment.

Prioritize business continuity risks

Once you have identified all business continuity risks in your organization, the next step is to assign weights to each of these risks based on how vulnerable your organization's data is to them and the level of impact they are expected to have on business continuity. Thus, you will be able to classify all the identified risks into 'high,' 'medium,' and 'low' categories. As can be expected, the category 'high' would consist of all risks that are likely to have the most damaging impact on your organization's business continuity. With this kind of classification or ranking system, you can automatically assign priorities to all the identified risks.

Perform a vulnerability analysis

By now, we know that it is important to know the business continuity risks in your organization. However, it is equally important to know how vulnerable your data assets are to each of these risks. Vulnerability is governed by the nature of the data that is being generated, shared, or processed in your organization and the efficiency and thoroughness of the security framework currently functional in your organization.

Employ risk prediction techniques

Since the cybersphere changes so rapidly, new security threats keep showing up at your doorstep every hour. Therefore, it is important to not only identify known risks but also discover and even predict new current or future risks that may affect your organization's business continuity. Automated algorithms can help you figure out new risk patterns, viruses, and other malware that cybercriminals may use to intrude into your organization's data assets.

Learn from previous data breaches or losses

'Learn from your past mistakes' is an important adage that many people follow in their lives. This is just as important in ensuring business continuity in your organization. Any past events of security breaches, unauthorized access, data losses, device malfunction, etc. in your organization should be used as the guiding light for designing new policies. This is an important aspect of business continuity risk assessment.

Do not forget to highlight any instances of non-compliance

As we mentioned in the previous section, your employees can greatly impact the security posture and business continuity of your organization depending on the extent of their compliance with security policies. In fact, quite often, compliance rules can also be extended to third-party vendors and applications. In your business continuity risk assessment, you must detect and highlight all instances of non-compliance in your organization.

Formulate a business continuity risk remediation plan

Risk assessment is not limited to identifying and ranking the business continuity risks in your organization. You must also design a business continuity risk remediation plan that is able to help you contain or eliminate all the risks you identified. It should be an efficient, easy-to-understand and easy-to-implement plan that is accessible to your security team as well as any other stakeholders in charge.

To manage the business continuity risks in your organization, start with the risk assessment steps that we have described above. In the next section, we discuss the ways in which you can perform the remediation of all the business continuity risks identified during the risk assessment.

Remediation of Business Continuity Risks

So far, we have looked at the kinds of business continuity risks that organizations face and the way in which these risks must be assessed. Once you have identified the risks to your organization's business continuity, the next step in the risk management workflow is risk remediation. Let us look at what you can do to remediate the business continuity risks in your organization.

Communicate with your security teams, third-party vendors and other stakeholders

One of the first things you must do when a risk becomes live is to communicate the issue with all your security teams. This becomes particularly important if your organization runs its business in multiple geographical locations. They must be instructed on how to pursue and attack an incoming risk by employing the necessary remediation measures. In case the risk you are dealing with is a third-party vendor risk, you are required to share the details of the risk and its impact with the concerned third-parties as well. They may, and ideally should be able to guide you out of a tough security risk caused by their products or services. In certain cases, you might also want to communicate with your customers to let them know what they can do at their end to restrict a certain risk. Moreover, if your organization is regulated by federal or state laws or industry standards, you may be required to share all the information about the data breach with the respective authorities too.

Control access to your data

Unauthorized access to your organization's data assets is one of the largest ways in which cybercriminals compromise your business continuity. One of the first things you must do when remediating business continuity risks in your organization is to check who has access to compromised data. Among those who had access, find out who shared the data, inadvertently or otherwise, with a possible cyber-criminal. Once you figure this out, you must regulate the access to sensitive customer or employee data very tightly. Change access authorization to a 'need to know' or 'required personnel only' level. Employ better password protection and encryption if necessary. This will prevent any further malicious penetration into your data assets. If you do not use a two-factor authentication system already, consider implementing it in all the departments of your organization.

Follow your risks and remediation efforts in real-time

Since new risks are generated so rapidly in the current age, it is important that you conduct a real-time analysis of risks and remediation efforts in your organization. Real-time monitoring of business continuity risks and remediation is possible only when you and your security team are aware of the current security posture and vulnerabilities of your organization. This will prevent any delay in containing or eliminating the risks that endanger your organization's business continuity. Moreover, this will prevent the risks from evolving into bigger threats with time.

Ensure compliance with risk remediation policies

Simply designing a risk remediation policy is not enough. You will also need to ensure that your organization's employees and even the top-tier staff abide by the rules and regulations written out in the policy. When everyone is compliant with security policies and remediation plans, chances of a risk penetrating your security barrier are very low. Thus, compliance is crucial to the success of any business continuity risk remediation and management program.

Keep up with new developments in the cybersphere

As we have mentioned before, both security technologies and cyber risks are evolving at a great pace. Therefore, it is important to not only keep up with the current developments in risks and security but also go beyond current knowledge by trying to predict new cyber risks that could take form in the future. Updating your team's expertise and experience is one way to constantly increase your organization's know-how in this field.

Secure all your physical data storage devices

If the business continuity risk that you are dealing with is a physical security issue, you must engage your physical security staff across locations to secure your physical data storage devices. This could mean adding an extra layer of protection or containment for your hard drives and servers, shutting down your systems to prevent electrical failure, creating necessary back-ups of your sensitive and important data to prevent data loss, or shredding documents that contain private customer information that can be misused by thieves or robbers.

Address issues with container security

If you identify the business continuity risk to be related to container security, your remediation efforts will depend on whether the container or applications in question were developed in-house or purchased from third-party vendors. If the container or applications were developed by the IT team in your organization, they will have to check the container image sources as well as the host operating system as these are the most vulnerable components of any container. Addressing the issues with container security will ensure that your container-related business continuity risks are remediated promptly.

Risk reassessment

The remediation of business continuity risks does not end with the containment or elimination of risks. You must also perform a reassessment of the remediated risks to know if there are still any security gaps or vulnerabilities in your security system that must be addressed. If this is not done, an eliminated risk can come back to haunt your business.

In this section, we have discussed some of the early steps you must take to remediate business continuity risks in your organization. In the upcoming section, we will discuss why it is beneficial to integrate your organization's business continuity risks with remediation.

Integrating Business Continuity Risks with Remediation

We have individually discussed business continuity risks, their assessment and their remediation. However, when a business continuity risk management plan is in action, it must work like a well-oiled machine – smoothly and efficiently. For the risk management machine to work well, the three components of risks, assessment and remediation must work like interlocked cogs. This can be achieved by integrating business continuity risks with remediation. There are several ways in which organizations can perform the integration of business continuity risks and remediation. Let us look at some of them.

Make integration a part of business continuity risk assessment

As we have discussed before in this book, business continuity risk assessment is the first step in an organization's security management workflow. One of the key steps of risk assessment is to allot the right measures to remediate a selected risk. This organically links business continuity risks with remediation. Thus, make integration of risks and remediation a part of the business continuity risk assessment in your organization.

Improve the visibility of business continuity risks and remediation

Undertaking any remediation efforts in an organization requires that the business continuity risks and the progress of any ongoing remediation operations be visible to the security team and other stakeholders. Higher visibility gives you a chance to separately assign a remediation plan for every single risk, thereby integrating risks with remediation.

Ask your security team members to answer relevant security questionnaires

Questionnaires provide a unique way to understand the state of your organization's security posture and business continuity. You can ask your security teams and other staff members to answer well-designed questionnaires that ask them about the risks, vulnerabilities, and remediation efforts in your organization. These questionnaires serve to increase the visibility of risks and remediation in your organization, thereby making it very easy to integrate them with each other.

Reassess your organization's vulnerabilities after risk remediation

As we have mentioned before, risk reassessment is an important component of remediation. In this process, you go through each of your remediated risks, match it with the remediation measures that were used and think of what needs to be changed to ensure complete elimination of the risk. This workflow naturally integrates all your business continuity risks with remediation.

Integrate third-party vendor risks with remediation

Since third-party vendors pose the greatest risk to an organization's business continuity, it is important to address them separately here. You must integrate third-party vendor risks with their corresponding remediation measures. This will require communication with third-party vendors to ensure that their remediation policy has good visibility for the employees in your organization. The integration of third-party vendor risks with remediation is also an important way to

automatically integrate application security risks with remediation in organizations that purchase their applications from third-parties.

Do not forget to integrate the applications developed within your organization

If yours is an organization that develops many or all of its business applications in-house, you must not forget to integrate the risks associated with these applications with their corresponding remediation measures. For this, the IT team must integrate risks and remediation in the development stage of the application itself. The developers of an application would best know the unique blocks of code in their applications that are often targeted by hackers and intruders. Moreover, they can perform a risk and vulnerability evaluation of their applications during the various stages of development such as design, test runs, and the final launch. When you integrate your application security risks with remediation, it takes you a step further towards integrating all your business continuity risks with their corresponding remediation methods.

Automation makes integration easier

When there are so many risks and distinct remediation measures listed out in your information security policy, manual integration of risks and remediation will seem to be a mammoth task. Luckily, developments in information technology allow us to automate these efforts. Automated platforms can help you immediately prioritize your risks and remediation, link risks with remediation, increase visibility, allocate the necessary resources for integration, enables a questionnaire-based analysis of your organization's security posture and business continuity and so on. One such platform that takes care of the integration of risks and remediation is BizzSecure's EAID solution. In the upcoming section, we will discuss the features of the EAID solution that make it so apt for business continuity risk management in any organization.

In order to secure your organization from business continuity risks in a swift and efficient manner, it is a great idea to integrate business continuity risks and remediation. Follow all the steps that we have listed above to integrate business continuity risks with remediation. Read our next section to know why BizzSecure's EAID solution is the best for business continuity risk management in your organization.

BizzSecure's EAID Solution Makes Business Continuity Management Easy

Thus far, this book has focused on the steps in the business continuity risk management workflow. We have discussed all the subtasks involved in business continuity risk assessment and remediation, the two essential steps to ensure business continuity. When one thinks of the pressure that these tasks exert on information security teams in organizations, business continuity risk management may appear to be a tedious and expensive operation.

However, what if we were to tell you that there is a way in which you can conduct all the tasks that we have described in this book on a single robust and cost-effective platform? BizzSecure's Enterprise Assessment and InfoSec Design (EAID) solution is the one-stop platform for all organizations to manage their business continuity risks in an inexpensive and efficient manner.

Let us take a look at the various features of the EAID solution that make it so apt for business continuity risk management.

It addresses all kinds of business continuity risks

At the beginning of this book, we talked about the different classes of business continuity risks – including network security risks, application security risks, physical security risks, third-party vendor risks, compliance risks and such. BizzSecure's EAID solution addresses all these classes of risks through a single software portal.

It makes business continuity risk management an automated process

The best part about using the EAID solution is that it automates your entire business continuity risk management workflow. This makes it so much easier to undertake the different steps in risk management, including risk assessment and remediation. Automation takes off your burden of religiously pursuing the innumerable subtasks that are a part of business continuity risk management.

It saves you time

When done manually, the different steps in business continuity risk management can be extremely tedious and time-consuming. Now, the EAID solution, as we have already mentioned, is an automated all-in-one platform. Therefore, one of the greatest benefits of using this portal is that it saves your organization a lot of time. Think of the person-hours you will save by using the EAID solution instead of assigning the same security management subtask to a member of your security team who should be spending their work time on something that cannot be automated easily.

It reduces both financial and human resource overhead

The work that goes behind each of the steps in business continuity risk management discussed in this book can prove to be very expensive for your organization if pursued manually. Moreover, it will require several person-hours, and thus, a lot of your organization's human resources. On the other hand, the EAID solution simply requires an affordable monthly subscription to readily take over the task of business continuity risk management in your organization. Since it is automated, you can also use your human resources to finish other pressing tasks in your organization.

It integrates risks with remediation

We have already talked about how important and beneficial it is to integrate business continuity risks with remediation in any organization. We also discussed the various steps one could take to perform this integration. The EAID solution helps you undertake each of these steps on its automated, holistic risk management portal. Thus, integration of business continuity risks and remediation is a lot easier with the EAID solution.

It generates quick and comprehensive risk reports

When you have so many kinds of business continuity risks to assess and remediate, generating reports of your analyses can be a cumbersome job. At the same time, these reports are important as they must be shared with concerned stakeholders in your organization such as the executives or the board of governors. You may even have to share them with third-party vendors and your customers depending on the kind of risks your organization is facing. The EAID solution helps you create well-informed and easy-to-understand reports about your organization's business continuity risk management operations. Such reports can be quickly shared with everyone in your organization.

It helps you prioritize business continuity risks

As we have already mentioned earlier in this book, an important step in risk assessment is to assign priorities to the risks based on their expected impact on your organization's business continuity. This is easily done through the EAID solution. Using the EAID platform, you can assign a weight to each risk depending on your vulnerability and impact analyses. This helps the software rank all business continuity risks automatically, thus setting your priorities for you.

It enhances the visibility of business continuity risks and remediation

In order to carry out a business continuity risk management plan effectively, it is important the two most important components of the plan, namely, risks and remediation, be completely visible to your security team as well as any other concerned stakeholders. The EAID solution increases the visibility of risks, risk assessments, and remediation efforts by authorizing selected individuals in your organization to fill out questionnaires pertaining to each security risk. When previously hidden risks become visible, risk remediation becomes both more prompt and more effective. Thus, the EAID solution makes your remediation process better by improving visibility.

It helps allocate resources transparently

To ensure the success of any business continuity risk management operation, proper allocation of resources, both financial and human, is necessary. The EAID solution greatly improves the visibility of your organization's resources and lets you allot them to a given risk remediation task when required. It also helps generate resource allocation reports for approval from the higher authorities.

It lets you compare your business continuity with reports from previous years

Since the EAID solution is an automated platform, it keeps a record of all the risk assessments and remediation efforts undertaken in your organization over several years. This gives you a unique opportunity to compare the current state of your business continuity with the state in previous years. You can also quickly generate comparative reports to properly and thoroughly analyze the maturity of your business continuity risk management planning. This way you get to learn from your previous risk management plans and mistakes.

Clearly, the EAID solution offers innumerable benefits to the organizations that subscribe to it. You can start using it in your organization now to streamline and automate the management of business continuity risks in your organization.

Conclusion

Security management is an indispensable task that all organizations handling any amount of sensitive customer or employee data must undertake. Lapses in security plans can lead to leakage, loss, and misuse of your organization's data, ultimately leading to financial losses and hindering your business operations.

To many organizations, this task may seem like a diversion from their actual objectives. Diversion or not, it is extremely important to manage and mitigate any and all risks that endanger the security posture and business continuity of your organization. However, business continuity risk management is not a trivial task by any means. It is lined with numerous subtasks that you must carefully pursue in your organization to ensure the core of your business operations remains unharmed in the event of a security risk penetrating your security barrier.

Through this book, we hope to have communicated to you the different types of business continuity risks that organizations face, and the ways in which such risks can be managed. We focused on two important aspects of any risk management plan – risk assessment and risk remediation. We also talked about the importance of integrating risks and remediation, and how this can be achieved in your organization.

Lastly, we provided detailed information on BizzSecure's EAID solution that has the capability to meet all your business continuity risk management related needs. We discussed the various features that make it apt for business continuity risk management in any organization. Hopefully, you found this information useful and are planning on subscribing to BizzSecure's EAID solution to ensure a smooth, efficient and prompt management of business continuity risks in your organization.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com