BizzSecure
PEACE OF MIND FOR InfoSec

Integrating Physical Security Risks with Remediation

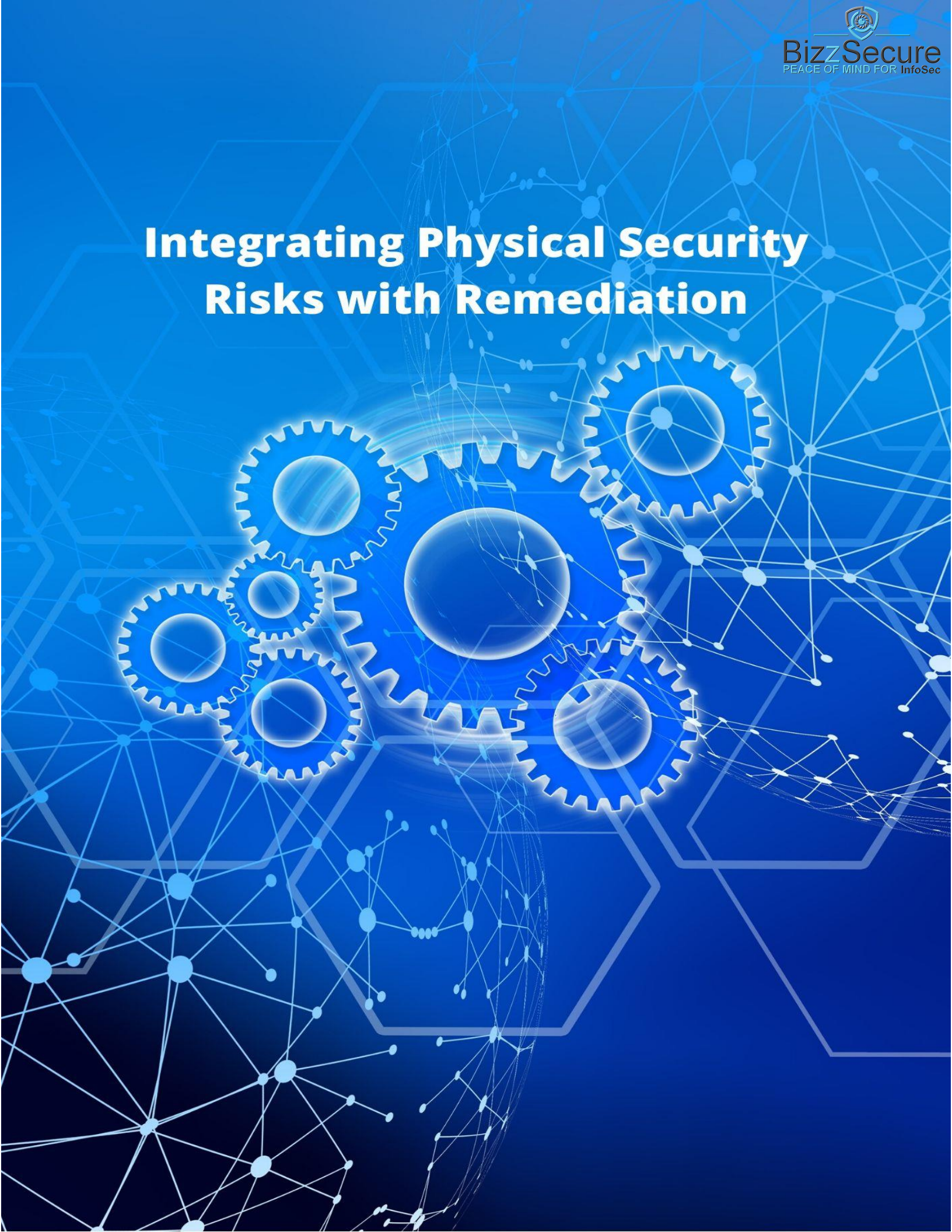

Table of Contents

Introduction

Handling some kind of customer or employee data digitally is a job that all organizations need to do in the current age, even if they did not set out to do so. As the world has grown into an increasingly digital entity, malicious actors around the globe have come with new ways to intrude into people's privacy and security. Organizations with any data assets have become key targets of such hackers. However, digital data can come into harm's way even without these online hackers. There is an entire class of security risks that are not dependent on any network or cloud to damage your data. These are called physical security risks.

Physical security risks could pose direct or indirect threats to your data by damaging your organization's physical infrastructure, breaching the security of your organization's premises, affecting one or more of your organization's different geographical locations, etc. Unfortunately, physical security risks are often underrated in many organizations dealing with data. This is usually a result of the false belief that data security only pertains to the digital security of information.

Physical security risk assessments and remediation are, therefore, just as important for securing your organization's data assets as information security, vendor, and compliance risk assessments and remediation. Moreover, just like any other kind of security risk, physical security risks must also be remediated or mitigated promptly to maintain the security posture of your organization. Prompt remediation of physical security risks requires tremendous visibility of both the risks and their corresponding remediation measures. It also requires a quick allocation of resources when remediation needs to be undertaken. All these requirements are automatically met when you integrate physical security risks with remediation.

The purpose of this book is to guide you through the needs and ways of integrating physical security risks with remediation in any organization. Before we go into the why and how of integrating physical security risks and remediation, there are three prerequisites that we would also cover in this book – (1) physical risks and their types, (2) physical risk assessments, and (3) physical risk remediation measures. Let's get started.

Physical Security Risks to Data in an Organization

Physical security threats can cause serious damage not only to your data assets but also to several other aspects of your organization's physical infrastructure. Just like there could be several kinds of information and network security risks in any organization that handles data, there is also a wide variety of physical security risks that can affect an organization's data assets. These effects could be direct or indirect, depending on the class of physical security risks in question. So, what are the different categories of physical security risks that organizations face in this age? Let us take a look.

Natural hazards and disasters

Each year, many natural hazards and disasters occur all over the world. These include earthquakes, hurricanes, floods, excessive snowfall, and forest fires among many others. No matter what the disaster, if your organization or its business operations are located in the eye of any such disaster, your data assets are bound to be affected in one way or the other. There are two primary ways in which these hazards endanger your organization's data assets: (1) they pose a risk to your premises or physical infrastructure, and (2) they threaten to damage your information security infrastructure. For example, in situations when internet connectivity is severely impacted due to a disaster, data in the process of being uploaded to or downloaded from a cloud or a server may be affected. The impact can be especially harmful if access to the data is limited to a fixed amount of time. On the other hand, there may also be direct damages caused to your physical data storage equipment such as hard drives or servers.

Human hazards in your premises

Your organization may also be at the risk of certain human hazards such as thefts of data storage equipment and devices by malicious intruders who may have gained unauthorized access to your premises. There may also be other human-made hazards such as intentional attempts at arson in your organization's premises to incur huge damage to your data storage systems. The extent and rate of these human hazards depend largely on the law enforcement and rate of crimes in the physical location where your premises are present.

Hardware damage and malfunction

The devices that help store your data assets can get damaged due to technological incidents beyond your control. Perhaps there is a surge in voltage one fine day, and your systems break down. Or, there could be a sudden electrical fire that damages your devices. These and other such incidents pose great physical security risks to your organization. If your data storage hardware, be it external or internal, does break down and you do not have any backups of your data, you may be facing huge losses of important information that was collected painstakingly over a long period of time. Hardware damage or malfunction could also include damage to the functioning of CCTV cameras that are meant to protect your organization's premises and property from intrusion, thefts, and damages. Non-functioning cameras could mean insufficient protection against human hazards. Due to the various reasons mentioned above, hardware damage and malfunction are among the commonly listed physical security risks in organizations.

Document thefts

It is possible that in addition to maintaining digital records of sensitive customer information, your employees sometimes print out this information for immediate use or analysis. However, these documents can become a source of great physical security risks to your organization. They can be stolen by unauthorized personnel or third-parties visiting your premises. They may easily be misplaced, and private information can get exposed.

It does not matter which of the above listed physical security risks your organization is facing. Anyone of them is equally potent to bring down your information security infrastructure. Therefore, you must take appropriate security measures to protect your organization from these physical security risks. The first step in this direction is to perform a physical security risk assessment. In the next section, we are going to discuss the different steps you should take to perform a physical security risk assessment in your organization.

How to Perform Physical Security Risk Assessment

Physical security risks are easily forgotten in organizations that handle data digitally on a regular basis. However, it is wrong to assume that digital assets are free from physical security risks. We have already discussed the various kinds of physical security risks that the data in your organization may face. Now, when you assess the strength and integrity of your organization's digital information security system, do not forget to complement it with a thorough evaluation of each of these different kinds of physical security risks.

Here are some steps you should follow in order to perform physical security risk assessments in your organization.

Identify all the physical security risk factors

In the previous section, we discussed what physical security risks constitute. To evaluate the physical security posture of your organization, it is crucial that you first analyze what specific risks your organization can be facing. The answer to this question will depend on where your premises are located, how accessible your workspace is to unauthorized people, nature and training of your security staff, the natural disaster risk zone that your premises are located in, the crime rate in your area and other such location-related questions. There will also be some storage device-related questions, such as from which vendor your external hard drives were purchased, or how well your hardware is placed on the premises. List out all these factors and rank them based on the probability of and the impact associated with each risk.

Evaluate your current physical security policy based on risk identification

If yours is an established organization with existing security policies, you must reevaluate your current security management system on the basis of the security risk factors identified above. This will ensure that any previously overlooked risks are covered in your remediation plans. Check if each of the risks identified above has a corresponding remediation strategy associated with it. If so, then ask yourself if the vulnerability of your data assets to any of these risks has changed. Also, check if the ranking of any of the risk factors has changed compared to the previous physical security risk assessments in your organization.

Compare physical security risks across different physical locations

As we mentioned in point about risk identification above, you will have to ask yourself a number of questions related to the location of your organization's premises. Now, an important part of a physical security risk assessment is to evaluate if your organization's business operations in diverse physical or geographical locations face different kinds of physical risks. Since these risks may vary in their type and intensity, it is important to compile the assessment reports from all locations in a single document. This will ensure that all the risks associated with different physical centers or units of your organization are visible to your central security team.

Assess the safety of your data storage devices

Your organization may be full of several data storage devices including computers, external hard drives or servers. An important part of ensuring the physical security of your organization's data assets is to keep these devices secure. During the risk assessment, check if your data storage devices are protected from excess sunlight, water, or dust based on the manufacturer's instructions. Monitor if they heat up excessively during regular operation. Keep track of any physical measures that your employees have taken to protect these devices. These assessments will help you analyze your physical security framework in a better light.

Backups

An important way to ensure that your data is never lost, or is easily retrievable if lost, is to create multiple backups. These backups should extensively feature in your physical security risk assessments. Are all your main computer systems regularly backed up? What kind of anti-virus protection is installed? Do your employees keep a log of the backup dates? Such questions will help you understand the extent and impact of any potential physical security risks that may damage your main devices or your backup drives.

Evaluate the security of shared office spaces

There are several business instances where multiple companies or organizations share a common floor or building. In such cases, it is important that you be extra careful with the security of your own part of the premises. During the risk assessment, check if your CCTV cameras are functional and positioned in the right spots. Check if there are unauthorized visitors entering your premises from other organizations within the building or outside the building. Consider interviewing the security staff of the other organizations on your premises too. This will help you protect your data assets stored in external devices from unauthorized access or thefts and damages.

Several steps are involved in a physical security risk assessment. When trying to integrate the physical security risks in your organization with remediation, remember to first conduct an in-depth physical security risk assessment in your organization using the steps we have described above.

How to Remediate Physical Security Risks

As we now know, sometimes, despite an organization's existing information security measures to protect its digital data, physical security risks present themselves. Remediation is the contingency plan that organizations develop exactly for such situations. Remediation steps are designed to eliminate any security risks that may have penetrated the security barrier in your organization.

Here are some steps to take in order to remediate physical security risks.

Develop a remediation plan

Some organizations may think that handling physical security risks is very unlike dealing with information security risks. They may think that since many of the physical security risks are not properly controllable, they cannot be appropriately remediated. Nothing could be further from the truth. It is important to develop a remediation plan for physical risks too. Think of each of the physical security risks that the different units of your organization face and design a remediation plan that addresses every single one of these risks.

Communication is the key

Physical security in an organization cannot simply be under the purview of any one department. Instead, it requires inputs from multiple departments. These include your security staff safeguarding your organization's premises, the technicians who monitor your CCTV camera recordings, the vendors who have sold you your data storage devices, etc. In fact, they also include organizations and institutions that are not even a part of your organization – such as the national weather service, the federal emergency management agency, etc.

Accountability and authorization

In the event of any disaster, accountability becomes paramount to risk remediation and mitigation. Since a lot of parties are involved in ensuring the physical security of data assets in any organization, accountability is also dispersed. Ensure that you assign responsibilities to a team of experts who will be accountable for carrying out the physical security risk remediation plans. Authorize the trustworthy members of your security team to handle the physical security of multiple premises or units at the same time. This could include your chief information security officer or other similar expert members of your staff.

Keep track of government advisories

In the event of a natural disaster that threatens the physical security of your data assets, you must pay heed to government advisories, such as the federal emergency management agency's warnings and recommendations. These advisories are meant to keep you and your physical assets secure. Note that in the case of your organization, physical assets include your premises, your organization's hardware, computer systems, servers, and other physical data assets.

Follow third-party vendor instructions to protect the hardware

You must follow the safety instructions provided by the third-party vendors from whom you purchased your data storage hardware devices. Also, keep a track of the warranty of these devices.

As you follow the steps mentioned above to remediate the physical security risks in your organization, you can also make your physical security framework stronger and more robust by integrating the physical security risks with remediation. In the upcoming sections, we go over the needs, advantages, and means of integrating physical security risks with integration.

Why is it Important to Integrate Physical Security Risks with Remediation?

We have now discussed what kind of physical security risks can endanger organizations handling any kind of digital information. We have also discussed the various remediation measures that can be undertaken to eliminate several physical security risks. Given the level of impact such physical security risks can have on your organization's security posture and business continuity, it is important that physical security risks and remediation be tightly linked or integrated with each other to make your security policy effective.

Let us take a deeper look at why it is important to integrate physical risks with remediation.

It makes your physical security workflow more efficient

Integrating physical risks with remediation ensures that all the steps in the physical risk assessment and remediation workflows remain tightly bound to each other, thereby making the security workflow very efficient and robust. In other words, integration accurately aligns all your physical security risks with remediation.

It reduces financial and human resource overhead

When resources, both financial and human, are allocated judiciously for any physical security task, your organization and its employees can freely focus and direct the majority of their resources on everyday business operations. Therefore, the integration of physical security risks with remediation helps you reduce the financial and human resource overhead in your organization.

It helps you track the progress of remediation measures in real-time

Integration is essential if you want to efficiently monitor the progress of any ongoing remediation measures. Progress would include the timeline of the remediation efforts, the extent of improvement of your organization's physical security posture, as well as their impact on your security workforce and resources. It also helps you understand what else remains to be done in order to make your organization completely secure from further physical security risks.

It improves the communication of physical security issues

Integration also makes the communication of physical risk-related issues better. When the visibilities of both physical risks and the corresponding remediation efforts are high, it becomes faster and easier to prepare or simply generate reports on the physical security posture of your organization. Such reports can then be swiftly shared with the stakeholders in your organization, including the CXOs, board of governors and any other senior management, as well as the employees and customers if need be.

It makes the allocation of resources easier

It becomes easy to allocate financial and human resources for physical security risk remediation if risks are tightly integrated with their corresponding remediation measures. This helps you to understand exactly what is required of you in the event of any physical security threat to your

organization. Therefore, you can better allocate the financial and human resources required to complete a remediation task.

It saves you time

The integration of physical security risks with remediation makes your remediation actions both more prompt and more effective. This is because integration greatly enhances the visibility of not only the risks and the ongoing remediation efforts but also the resources allocated to each step of the security workflow. Together, these benefits of integrating physical security risks with remediation help your organization save a lot of time.

It helps you track compliance

With greater visibility of physical security risks and remediation, you can also easily track your employees' compliance with your physical security policy. Therefore, the integration of physical security risks and remediation allows you to monitor which of your employees or which of your departments first encountered a physical security risk and how. If some measures listed in your security policy were not followed, they will also become visible due to the integration of risks and remediation.

Therefore, integrating physical security risks with remediation is not only important but also provides several additional advantages to any organization. In the upcoming section, we discuss the different steps you can take to integrate physical security risks with remediation in your organization.

How to Integrate Physical Security Risks with Remediation

Hopefully, we have been successful in impressing upon you the importance and advantages of integrating physical risks with remediation in your organization. However, how does one go about integrating physical security risks with remediation in any organization?

Here are some steps you should follow to integrate physical risks with remediation.

Make integration a part of physical security risk assessment

Previously in this book, we have discussed the steps involved in conducting a physical security risk assessment. One way to integrate physical security risks with remediation in your organization is through physical security risk assessment. Since a physical security risk assessment requires that you identify and rank all the physical security risks in your organization, you can easily use this process to assign a remediation measure for any given physical security risk. This makes integration a part of your organization's physical security risk assessment.

Coordinate with government bodies

As we have discussed before, physical security risks related to natural hazards should be remediated by following government advisories on such matters. In such cases, remediation efforts inadvertently become a collaborative effort between your organization and the government agencies trying to protect people and property from the perils of natural disasters. When you coordinate with the government bodies that are helping you secure your lives and property, you automatically integrate natural hazard-related physical security risks with their corresponding remediation measures.

Reassess the risks that you have remediated

It can be dangerous to overlook the task of risk reassessment. Once you think you have remediated the physical security risks in your organization, perform a reassessment of all the physical security risks. Have they truly and completely been remediated? Are there still data assets that are vulnerable to these physical security risks? Do you need to amend your remediation measures based on a reassessment of physical security risks? Answering these questions will allow you to detect any remaining gaps in your physical security framework. This will help you integrate physical security risks with risk assessment as well as remediation.

Enforce compliance

Enforcing compliance of your employees with your organization's physical security risk management plan is critical to maintain your physical security posture. To enforce compliance, it is important that your employees have clear visibility and understanding of all the physical security risks as well as the remediation measures in your organization. Providing this visibility naturally integrates physical security risks with remediation in any organization.

Automate your physical security workflow

The processes of physical security risk assessment and remediation can get quite taxing and time-consuming if done manually. This is particularly true when your organization has multiple different branches located across various geographical locations. Moreover, manual integration would also consume more financial and human resources, thus diverting these resources from the primary objectives of your business operations. Automating your security management workflow can help you out in this situation. Automation also helps improve the visibility of your organization's physical security risks and their remediation across all the physical locations where your operations are conducted. Once all your physical security risks and remediation measures are visible, it becomes easy to integrate the two.

How can BizzSecure help?

BizzSecure's EAID solution provides an integrated, all-in-one platform to help you meet all your information and physical security needs. All the steps for integration of physical security risks with remediation discussed in this section are easily achieved through the EAID solution. With a monthly subscription of the EAID solution, you can easily automate the integration of physical security risks with their assessment and remediation. The next section is dedicated to a detailed analysis of all the advantages that the EAID solution provides to any organization for integrating physical security risks with remediation.

Using BizzSecure's EAID Solution to Integrate Physical Security Risks with Remediation

In the previous section, we discussed the various ways in which you can integrate the physical security risks in an organization with their corresponding remediation measures. However, it is important to understand that the manual integration of physical security risks with integration can be tough and tedious. Moreover, since it is unavoidable human nature to make errors, you may even miss out on one or the other important aspects of integration when you go the manual route. Therefore, it is best to undertake the integration of physical security risks with remediation through an automated platform.

BizzSecure provides a great way to automate the integration of physical security risks with remediation – the Enterprise Assessment and InfoSec Design (EAID) solution. This all-in-one software solution automates and integrates all the processes of security risk management into a single portal. Let us take a look at how BizzSecure's EAID solution provides several advantages while integrating physical security risks with remediation.

EAID solution enables judicious use of time and resources

Automation of integration through the EAID solution helps you save a lot of time and resources on the integration of physical security risks and remediation. Since it is all done through a common portal, you do not have to engage any additional members of your security team to perform the task of integrating risks and remediation. This also reduces the additional financial burden causes by manual integration of risks and remediation in any organization.

EAID solution enhances transparency in the physical security workflow

It also makes the integration process more transparent as each time, both the risks and remediation measures can be visualized simultaneously. Moreover, the EAID solution allows you to authorize any crucial stakeholders to visualize and analyze the physical risks and their ongoing remediation in your organization. These stakeholders could be the team that guards your security premises, people who monitor CCTV camera feed, employees in your information security team as well as the executive and board level staff. Transparency in the security workflow also increases accountability.

EAID solution improves risk-related communication across all your geographical units

An important aspect of physical security is the monitoring of security in premises set across all the units or physical locations of your organization's business operations. The integration of physical security risks and remediation also brings together the physical security aspects of these different business units in your organization. With an automated physical security workflow, you can immediately communicate with your security teams by providing them with thorough physical security risk assessments conducted across the different geographical locations of your organization. Since the risks and remediation measures will be integrated with each other, your teams will be able to quickly take remediation action against any physical security risks.

EAID solution lets you track remediation in real-time

The EAID solution allows all its users to keep track of their remediation efforts in real-time. This is true for physical security risk remediation too. Through real-time monitoring of remediation efforts, you will be able to follow which physical security risks are being remediated by which department, team, or unit of your organization in what amount of time. This way, the EAID solution allows you to judge how good your remediation plan is, while also naturally integrating physical security risks with their remediation measures.

EAID solution helps you track the maturity of your physical security framework

Physical security risks and remediation are integrated through the EAID solution, where you can also look at how these risks, their remediation measures, and the effectiveness of these remediation measures have tracked over the past several years. This allows you to analyze the change in the maturity of your organization's physical security risk management. Additionally, you can quickly generate, export, and share analysis reports through the EAID solution that can make a visual comparison and tracking of the maturity of your physical security framework a lot easier.

EAID solution integrates the security frameworks of all your geographical units

Your organization may be conducting its business operations in a number of different physical (or geographical) locations. Now, depending on the nature of operations in different physical locations, your security policies and requirements are likely to change. Therefore, tracking your security framework for several locations simultaneously may seem extremely tedious and cumbersome, and in some cases, will be impossible to do manually. Automation of physical security risk assessments and remediation comes to the rescue for such organizations that conduct multi-site operations. Automation allows you to simultaneously take a look at the information and physical security frameworks of all the physical locations where your organization's business is operational.

EAID solution improves risk and remediation visibility across locations

It is important to get a holistic view of all the physical security risks faced by different regional centers of your organization. At the same time, each individual physical location also needs its own distinct review of physical risks and remediation so that the teams in charge of physical security can take appropriate action at their own location. When you integrate physical security risks with remediation on the EAID portal, you can authorize the concerned team members in your organization to get real-time visibility of physical security risk assessment and remediation across all the geographical locations where your business operations are conducted. Moreover, since you can look at the physical security risks that threaten your organization as well as the corresponding remediation measures that can get rid of these risks on the same platform, you can easily integrate physical security risks and remediation through the EAID solution.

Given the sheer importance of integrating physical security risks with remediation in all organizations handling customer or employee data, automation of integration through BizzSecure's EAID solution could be the much-needed tool your organization needs.

Conclusion

The physical security of data assets is an often-overlooked aspect of information security in any organization. However, it should be among the top priorities on your list. Remediating physical security risks in your organization is a must to maintain your security posture.

For any physical security risk remediation effort to be viable, it must be prompt and to-the-point. This is indeed also true for physical risk remediation. Since physical risks pose a huge risk to your organization's finances, it important to invest time, money, and resources into planning a physical risk remediation strategy. Investment and allocation of resources must happen at the right time and in the correct proportions. Moreover, such remediation efforts should have high visibility to prevent or reduce any damages to the organization's data assets.

The only way to ensure that all of the above tasks are executed in the wake of a physical security disaster is to integrate physical risks with remediation. Integrating physical risks with remediation is an important step to ensure that risks get identified and remediated in a prompt and efficient manner.

Through this book, we hope to have answered the following questions: (1) why is it important to integrate physical security risks with remediation, and (2) how can organizations integrate physical security risks with remediation? Along our way to answering these specific questions, we also discussed some indispensable concepts such as the different types of physical security risks that typically endanger different organizations, what a physical security risk assessment entails and how physical security risk remediation is conducted. Towards the end, we also put special emphasis on the numerous ways in which BizzSecure's EAID solution can help your organization solve the problem of integrating physical security risks with remediation.

Overall, we hope that this book could emphasize the importance, advantages, and ways of integrating physical risks with remediation. Consider subscribing to BizzSecure's EAID solution to perform physical security risk assessments, remediation and integration of physical security risks and remediation in your organization among several other information security-related tasks.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com