BizzSecure
PEACE OF MIND FOR InfoSec

The Importance of Integrating Security and Compliance Risks with Remediation

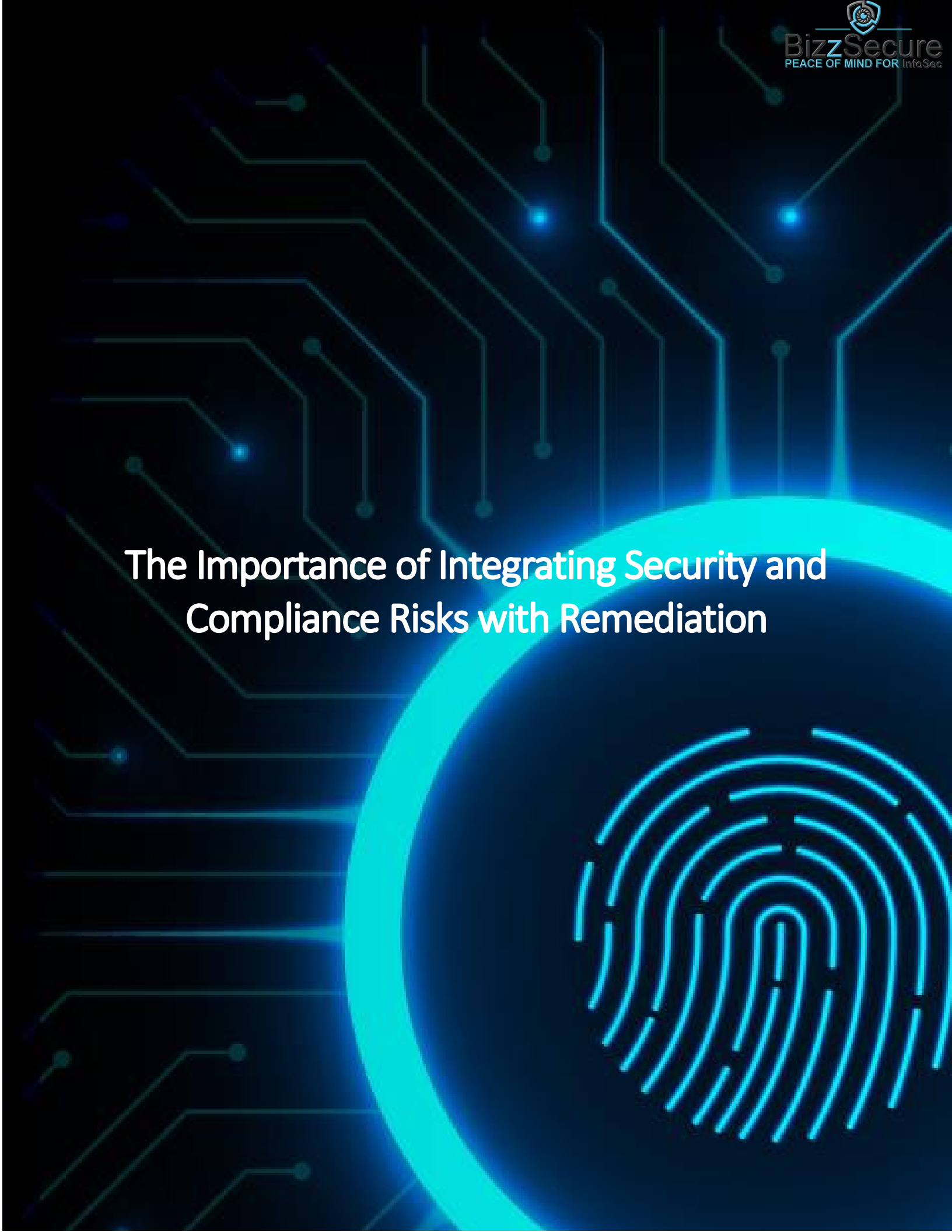

Table of Contents

Introduction

The world of business faces challenges when it comes to safeguarding any organization's data. Maintaining a business' security posture has, and always will be, an ongoing fight with new risks crowding the cyber-sphere every passing minute. As cyber-criminals get smarter with assistance from information technology, they get more and more dangerous to businesses.

It gets more horrifying as you go through the results of PricewaterhouseCoopers' 2018 global economic crime and fraud survey. According to this survey, less than 50% of the world's organizations conducted a cyber-crime risk assessment during the two years before the survey was conducted. Unfortunately, according to the same survey, cyber-crime is one of the most reported frauds in organizations around the world. In fact, it was found that organizations spent twice the amount that they lost through cyber-crimes on investigating and conducting interventions for these crimes.

Moreover, the sources of these risks and threats to your organization's data are not limited to people outside of your business. You may discover that people within your organization have unknowingly and unintentionally exposed your data to damaging risks. We know that it is not a comforting thought, but it is an honest view of the security risks endangering any organization.

It is easy to believe that someone outside your organization is trying to bring it down by threatening your data assets through technology. However, how can your own employees elevate the risks you face? The answer is non-compliance with security policies and regulations. It is important to understand and acknowledge that compliance is an integral requirement when it comes to securing your organization's data assets. Isolated instances of non-compliance may seem irrelevant in the beginning, but they can lead to massive leakage or theft of sensitive data. In cases where businesses are regulated by federal or state laws, there can be sizable financial losses in the form of penalties and in clientele due to a lack of trust. In extreme cases, one should be prepared for legal proceedings too.

Given how crucial compliance is to ensuring information security, it is not surprising that a lot of organizations invest a significant portion of their time and resources establishing good information security policies and ensuring compliance by their employees. Nevertheless, businesses still tend to face issues of non-compliance and security risks.What should you do if there are some inadvertent and uncontrollable cases of non-compliance and security risks? A plan for remediating the threats is vital in such grave scenarios.

As expected, remediation is meant to counter the threats faced by your organization. Any measures that can protect the security posture of your organization are part of the remediation plan. However, the steps to be taken for remediation depend on the kind of risk. An intensive assessment of security- and compliance-related risks can help you classify the various potential risks at your organization. Each of these risks to your data assets can then be connected to a set of remediation measures that should be adhered to in the event of a security breach. This link between risks and remediation exists not by design, but by default due to the very nature of the two. The link between risks and remediation is valuable to organizations because it can make risk assessments and prevention more effective, more streamlined, and less resource consuming. Therefore, it is

important that organizations preparing remediation plans integrate them with the security and compliance risks specific to their business. Cyber-risk remediation analyses and automation of risk assessments and remediation are effective ways to bring about the integration of risks and remediation.

With this book, we want to draw everyone's attention to the importance of integrating security and compliance risks with remediation. We provide an insight into what it takes to integrate security and compliance risks with remediation. We start with what events count as security and compliance risks. We also provide some tips to conduct security and compliance risk assessments. We further elucidate why quick remediation measures are vital to your business operations. Lastly, we discuss the importance of, and the different steps required for, integrating risks and remediation.

Types of Security Risks

Put simply, security risks include any threats to your organization's security – whether digital or physical. Digital or information security of your organization's data depends largely on the measures that work towards safeguarding your network. The internet makes your data assets susceptible to various kinds of risks while surfing the web or sharing data within or outside your organization or even storing data on a cloud that is not secured.

On the other side, there are also physical security risks that can affect your organization's data. These risks affect the physical, tangible devices or servers that allow you to store or share your data. Now, a large number of physical security risks may not be directly under your control. For example, natural disasters such as earthquakes, floods or hurricanes are not under your control, even though some (like hurricanes) can be monitored and predicted with modern technology. Other physical security risks, such as robberies or thefts and fires are largely preventable with the right measures.

Let us look at some security risks that businesses typically face.

Some information security risks to your data

Malware

Malware, viruses, and spyware have mushroomed in the cyber-sphere in the past decade. With the development of new malicious software targeting sensitive data, new means of delivering that dangerous software have also been discovered and invented. Phishing emails, artificial intelligence-powered chatbots, and manipulated blockchain systems are only a few of the many relatively new ways in which fraudsters are propagating cyber-crime.

Data leakage

Hackers have their hawk-eyes upon your data all the time. Whether your data is associated with your customers or your employees, many threats are always looming large. Any intrusion or unauthorized access to your organization's data repositories can mean a massive leakage of sensitive and confidential information pertaining to your employees,your customers, or both.

Some physical security risks to your data

Natural disasters

Natural disasters and hazards such as earthquakes, hurricanes, floods, snowfall, or forest fires pose a risk to your infrastructure as well as data security structure. They can severely affect the internet, particularly in the events of power outages triggered by such natural hazards. This might affect the storage of data that was being uploaded to or downloaded from a cloud provider when a power outage transpired. Similarly, direct damages levied upon your data storage devices or servers due to these hazardous events cannot be discounted either.

Man-made hazards or mishaps

Apart from natural disasters, there are also man-made threats to your organization's data safety. For example, if unauthorized people gain access to your organization's premises, they could wreak havoc on your data storage devices and servers. Similarly, deliberate attempts at arson can damage your information stores as well as other infrastructure.

Hardware malfunction

If you are not in the habit of having your organization's data backed up in multiple places, you may be exposing your business to great risk in the form of potential hardware malfunction. This applies to all external or internal storage devices in your organization's computer systems. It also includes any servers. Hardware malfunction is not in any one person's hands. It can happen inadvertently and without any warning.

Compliance risks

Compliance with security policies is an area that could be a source of huge risks to your organization's data. When information and physical security policies are designed for any organization, the hope is that all employees would strictly abide by them. It can get difficult to enforce this if the policies are not written or explained in an easy-to-read, easy-to-follow manner. Some specific policies, usually ones where federal regulations are discussed, necessitate additional training. Lack of training means poor compliance, and poor compliance leads to complete failure of, or a devastating compromise in, the organization's security mechanism.

All the various risks discussed in this section must be assessed for their potency and possibility in the context of your organization's data operations.

Some Tips for Security Risk Assessments

Your organization's data can be exposed to various types of risk. The important question to ask is: how do you prevent them? To prevent any kind of security risk to your data, you must evaluate your business, the risks it may face due to its very nature, and how you may be able to keep these threats at bay. This is precisely what a security assessment is.

Information security risk assessment is the foremost step in establishing an impenetrable protective barrier around your data assets. Here are some tips one should follow when conducting security assessments.

Create a list of all kinds of data at your organization

Classify all the data assets that are regularly generated, shared or processed in your organization. The classification should be on the basis of the vulnerability of each data asset to a potential cyber-threat. This will help you assign risk values to the data later.

Foresee the impact

Take a long, hard look at how a security threat will affect your organization's business. Think of how data leakage would impact your customers and employees. Associating the possible impact with each potential risk is an important component of security risk assessment.

Risk discovery

Since security threats keep changing and are constantly updated, try to get ahead in the game. Use an IT expert in your organization, hire a third-party, or use security software to help you discover new threats in real-time. These new threats will be crucial to your risk assessment and remediation.

Always document your research

Your security risk assessment must be documented in the form of a report that can be shared with all stakeholders, both inside and outside your organization when needed. This way, it will be easier for them to be a part of designing the remediation plan for your organization.

Do not overlook previous incidents of risk exposure

Consider any previous security breaches at your organization a lesson in strengthening your security framework. Use them to design better security policies for your organizations. You already know the loopholes that were targeted by malicious entities in the past. You can use this knowledge to predict other vulnerabilities as well.

Check if your employees are all compliant to your security policy

Security is zero when there is no compliance. Ensure that your employees, even if they are high up in the food chain, are compliant with all the points elaborated in your security policy. Lapses in compliance should be documented in your security risk assessment.

Some Tips for Compliance Risk Assessments

Unlike security risks that are always changing with time, compliance risks are easier to avoid. In fact, a little investment of time and resources may even permanently eliminate compliance risks altogether. However, this requires the attention and good intentions of your entire organization. Employees stationed at all tiers need to adhere to the compliance plans set by your compliance officer.

As we have mentioned before, there are two types of compliance. You need to comply with federal and state laws and regulations concerning data security to protect your customers while also fulfilling your legal obligations. This type of compliance is usually easier to enforce as the word 'legal' carries and propagates an urgency that all employees understand. However, the second kind of compliance – one where your employees must strictly follow the rules set by one of their own – is a lot more difficult to implement. It requires goodwill, a sense of responsibility, a sense of duty towards the organization and its customers, awareness, and immense care. While we all hope that our employees will have all these qualities, it is extremely difficult. Therefore, a strictly enforced internal compliance plan becomes a necessity.

Here are some tips that you should follow when performing a compliance risk assessment for your organization.

Compliance plans should be based on risk assessments

Dealing with compliance risks requires you to identify, rank, and remediate them timely. Therefore, your organization's compliance plan must be devised on the basis of thorough internal security and compliance risk assessments. All security risks should be categorized and ranked based on their likelihood and impact on business operations. Similarly, failures in compliance must also be ranked and tagged based on the severity of their effects on your organization's security posture and business continuity. The compliance plan should put more weight on high security- and compliance-risk areas.

Include your employees in the formulation of compliance policies

One way to increase compliance among your employees is to make them a part of the formulation of security and compliance policies. This will help them gain inside information and better insights into the proceedings of risk assessments and requirements of the law and your organization. They can then easily identify aspects of their daily work routine that may be exposing your organization to risks. If their security software is outdated, or if they are surfing malicious web content, or perhaps if they are sharing company data with an untrustworthy third party, they would now be more careful.

Maintain distinct compliance reports for different policies

Compliance needs to be tracked on a regular basis, with reports generated and shared with all stakeholders. Since many organizations must also comply with federal and state policies on information security, specific compliance tracks must be created for separate policies. For example, if your organization is regulated by the Payment Card Industry (PCI) Data Security

Standards (DSS) as well as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), you should track their compliance separately albeit simultaneously. Separate compliance reports will make it easier for you to identify specific areas where your organization's compliance needs to be strengthened. It will also make it simpler to discuss issues related to compliance with federal or state auditors when they come knocking.

Compliance assessments between federal/state policies and your organization's internal policies should also be tracked separately. This is recommended because many features of your organization's information policy are likely to overlap with those enlisted in the policies of regulatory agencies. The overlap may blindside you towards maintaining adherence towards your own security policies. It can also give you a false sense of complacency even if only a few of the many points in your compliance plan are being followed.

Ease of understanding

This is probably the most underrated part of an audit report or compliance assessment. It is also, arguably, the most crucial one. If your employees find it difficult to understand the meaning of certain security policies or do not follow you when you talk to them about the need for compliance, your business may be in serious danger. Make your compliance reports more readable and comprehensible. In the end, your employees may all be very smart people, but that does not automatically mean that they will be willing to invest the requisite time into parsing a compliance report. Use infographics or even animation to get your point across to the stakeholders and slackers, if any.

Compliance reminders and training sessions

Regular reminders on compliance requirements would help refresh the memories of your employees and let them know that their performance is being tracked. Similarly, frequent training sessions would help them clarify any doubts about the compliance policy and the risks associated with non-compliance.

Compliance assessments can get tedious if not done the right way. Follow our tips to make compliance risk assessments more useful for remediation and mitigation.

Preparing Your Organization for Risk Remediation

It is always our hope that our current security measures are enough. However, we are often met with the harsh reality that the malicious opponents targeting our data are better than us. Sometimes, it does not even take an opponent or a malicious intent to bring a business down. An inadvertent failure to comply with a security rule by your own otherwise well-meaning employee can greatly undermine your overall security framework. Thus, security and compliance risks often come as a combined package.

Since information security is constantly challenged by new threats from outside or within an organization, any business can get exposed to security risks despite the extent of efforts put in to prevent them. It is for situations such as these that one must have remediation plans. Remediation measures can include any step that can limit and remove the threat to your data assets. Thus, remediation could involve updates to authorization for accessing data, fundamental changes in standard operating procedures, communication of threats to stakeholders, installation of security software, system shutdown, and alterations in system design among others.

Before we dive deep into how an organization should prepare for and conduct remediation when hit by a threat, let us clarify two terms. In the context of information security risks, the term remediation is often used with or in place of mitigation. Both almost always go together because they both refer to dealing with the threats at hand. There is a slight difference, however. Remediation is done when a threat can be completely removed from harming your organization. On the other hand, mitigation is the action taken when a threat cannot be eliminated completely but maybe pacified. Sometimes, you can only mitigate a threat at your end and then request your customer to take further steps to remediate it. No matter what term you use, both remediation and mitigation are key processes that help ensure business continuity.

So, how do we go about conducting effective risk remediation? Let us look at some of the important steps involved in preparing your organization for risk remediation.

Create an actionable remediation plan

Preparedness pays off well when you are in the middle of an ongoing data security threat. Create a remediation plan in case one of your security and compliance risks turns into a live threat for your organization. However, remember that the remediation plan you formulate needs to be actionable, practical, and foolproof. All your employees, and perhaps even your customers (if they need to partake in the remediation process) should be able to follow the plan to the letter.

Prepare your employees

Your employees are your most important assets – even above your customers arguably. Especially when it comes to information security. You must communicate any data threats that have penetrated your organization to your employees – honestly and promptly. You should also have them periodically revisit your organization's compliance plan so that they can immediately correct any of their mistakes that make your organization more vulnerable to future risks.

Bring together a back-up taskforce

It would be a good idea to keep a back-up team ready for remediation purposes. The sole intention of formulating such a team should be or them to take charge of remediation when a breach happens. This team should consist of trained IT experts and tech analysts. They should have permission and the freedom to formulate and update the remediation plan as required by a certain situation or development. In the event of a dire situation, this task force should also be in charge of communicating the requirements of remediation to all the stakeholders in your business, including your customers.

Keep a check on accountability

When it comes to compliance and security risks, accountability is extremely vital to the remedial operation. The employees tasked with information security in your organization must all be held accountable in the event of a network breach that threatens the entire organization. Their status or position in the organization should not matter. Remove all preconceived notions and biases when deciding and ensuring accountability. Whenever a breach happens, the people accountable for security operations in the organization are expected to take the lead and explain the reasons for the intrusion. This is essential to an effective remediation plan.

Conduct random security drills

Security drills are akin to disaster management drills or fire drills that are actively conducted in various organizations across the world. Conducting information security drills will help you prepare for the worst when it comes to a data threat. For example, advanced persistent threats can be simulated, and such simulations can be used to train the staff in your organization. You may even hire a third-party organization or vendor to help you simulate such a situation in your organization. Rate your security measures based on the outcomes of these drills. This will help you practice remediation. It will also aid in planning for better ways to remediate risk.

Remediation is any organization's last resort to save its business in the face of a security disaster. It, therefore, demands time, resources, and thoroughness from the stakeholders undertaking it. Follow the steps we have discussed above, and your organization will be in good shape to undertake efficient remediation measures.

Why is Integrating Security and Compliance Risks and Remediation Important?

We have now discussed in detail the kind of security and compliance risks your organization may be facing each day. We have also understood the importance of remediation and the ways to make it efficient. However, it is essential that we look at these two seemingly disparate things as a whole. There is no remediation without a security or compliance risk. Similarly, there is no risk if your remediation measures are impeccable. They must go together when it comes to maintaining any organization's security posture.

Let us discover the importance of integrating security and compliance risks and remediation.

Eliminate the perilous disconnect between risks and remediation

When a security threat strikes at your organization, you simply cannot afford to lose time. Swiftness in undertaking remediation measures is critical to the security posture of your organization at the time of any incumbent risk. Rapid interventions are only possible if you have a good and efficient remediation plan written out for different risks. Any plan to protect your organization's data will be both efficient and timesaving if you integrate the security and compliance risks with remediation. Integration leaves no room for error by eliminating any disconnect between aspects of risk discovery and assessment and the remediation measures that must be taken to deal with each risk.

You save a lot of financial and human resources

Integration also prevents unnecessary resource consumption in any organization. It will reduce the manpower needed to perform the otherwise segregated tasks of risk discovery, risk assessment, and remediation when a risk becomes a threat or worse. This, in turn, means that the extra financial resources that your organization would have invested in conducting these tasks separately would also be saved. Thus, the integration will help reduce the human and financial resources your organization dedicates for securing your data assets while making the security more effective and streamlined.

Discovering risks and implementing remediation in real-time

Security management is a continuous task because cyber-risks and cyber-criminals are continuously and spontaneously evolving. Therefore, if huge financial and legal threats are facing your organization due to an information security breach, you cannot risk for them to grow larger than they already are. The best way to evade such a situation is to detect the risks as they are encountered and to remediate them immediately. Integration of security and compliance risks and remediation allows you to discover and address cyber-threats in real-time.

Better compliance and security monitoring

The integration allows you to better monitor your organization's security and compliance as well as the associated remediation plans. This is because integration requires you to link each discovered or anticipated security or compliance risk to a countermeasure for risk remediation. You can keep a track of security and compliance risks and threats by discovering them in real-

time. Once a threat is detected, automated remediation procedures can be initiated without further ado. Once the threat is contained or eliminated, it becomes important to continue conducting security and compliance audits and evaluating their results. Comprehensive and self-explanatory reports should be generated based on the audit results. All these steps become naturally easier when risks and remediation are integrated with each other.

Integration makes automation easier

As IT has taken huge strides in developing useful tools to keep security risks in check, it is not surprising that software today can provide you all the details about security and compliance risk assessments and remediation measures with a single click. When you integrate remediation steps with the security and compliance risks the steps are addressing, you make it easier for the software to decide which remediation measures to follow when it automatically detects a certain risk. The usefulness of integration easing the automation process is enhanced by the fact that risk detection is happening in real-time as the software continuously monitors your organization's information security framework.

Your reputation is at stake

Remember, in the event of a data breach in your organization, apart from the obvious data theft and associated financial losses, you also stand to lose your reputation. In such situations, once again, swift remediation is key. This also includes immediate communication. Letting your customers, clients and employees know about the situation that has transpired in the organization is not only your duty but also their right. Give them pointers on what they can do at their end to minimize losses. Also, let them know what you are doing under your remediation plan. Quick communication will help control the situation, maintain your customers' trust and thus, uphold your reputation in the wake of a security disaster. The integration of risks and remediation allows you to do all of these things promptly and efficiently. Therefore, when your security and compliance risks and remediation are integrated with each other, you can successfully maintain your organization's reputation during a security system failure.

Given the many benefits of integrating security and compliance risks and remediation, all organizations should start their respective risk assessments with this integration process.

How to Integrate Security and Compliance Risks with Remediation?

Security and compliance risks and remediation cannot and should not be disjointed. To ensure that security and compliance risks are eliminated or remediated immediately, a useful method is to integrate risks with remediation. This book has already elucidated the importance of integrating security and compliance risks and remediation. Let us now look at how to perform this seemingly complicated integration.

Here are some steps your organization should follow to integrate security and compliance risks and remediation.

Security and compliance risk assessments go hand in hand

It is incorrect to think that security and compliance risks are distinct and exclusive. Any lapse in compliance is a serious potential security risk. They are tightly interwoven. Since the risks are linked to each other, so should the risk assessments. Perform security and compliance risk assessments simultaneously in your organization. One will guide the other. Assessing the security risk areas specific to your organization will help you determine the compliance policies you need to keep away any risk. Similarly, if you identify any compliance risks in your organization, it will also tell you what kind of threats your data assets can become susceptible to, allowing you to correct these as they arise. Therefore, to integrate risks and remediation, it is important to start by integrating security and compliance risks.

Make security and compliance your top priorities

This goes without saying, but security management should be high up on the list of priorities for your organization. If security and compliance are your top priorities, you will automatically perform the necessary risk assessments before assigning relevant remediation measures for each risk. You will try to be a step ahead of the crowd in ensuring that your data assets remain secure. This will undeniably require the integration of risks and remediation.

Cyber-risk remediation analysis

This is one of the most important and organic ways to integrate security and compliance risks and remediation. A cyber-risk remediation analysis allows you to select the remediation steps that will best counter an incoming or persistent threat. This involves painstaking efforts to determine the susceptibility of each of your organization's data assets to the threats that have been identified during the risk assessment. Based on the susceptibility to a given threat, a corresponding remediation step will have to be decided. Since threats and their corresponding remediation measures are so spontaneously linked to each other in cyber-risk remediation analysis, this becomes an important means to ensure their integration.

Automated risk discovery and remediation

Automation seems to make lives much easier in a lot of spheres. This is indeed true when it comes to securing your business. Thanks to modern information technology, it has become possible to automate both risk assessment and remediation. Security software can now allow you to digitally

integrate security and compliance risks in your organization with related remediation measures. As we have mentioned before, it allows for detection and remediation in real-time, thus making your security framework more robust.

Integrating security and compliance risks and remediation is not only important but also easy to do. Follow our steps and make your organization more remediation-friendly.

Conclusion

Every organization is simply unstoppable until that one overlooked and unexpected security threat presents itself. As we have learned through several sections in this book, you could be just as responsible for jeopardizing your organization's data as a malicious hacker sitting miles away on an internet network.

The keywords to prevent security risks here are compliance and remediation. Security risks, compliance risks, and remediation – the three are strongly connected to each other. Security and compliance risk assessments are integral cogs that drive each other. On the other hand, remediation is guided by the kind of security and compliance risks that organizations face. In order to ensure that your organization's security stays strong, impenetrable and robust, it is important to integrate risks and remediation.

Hopefully, the information encompassed in this book has helped you understand the importance of integrating security and compliance risks and remediation. We have first discussed the various kinds of information and physical security risks that threaten any organization's data. We have also briefly presented the types of compliance that your organization must ensure in order to protect its data assets. We then moved on to provide some tips on conducting risk assessments, followed by a discussion on the importance of integration and the ways to do it.

We sincerely hope that you are able to use your newfound understanding of the needs and means for integrating risks and remediation to improve your organization's security posture and overall data health.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com