BizzSecure
PEACE OF MIND FOR InfoSec

How the EAID Solution Empowers CISOs

Table of Contents

Introduction 3
Who is a CISO? 5
Role of CISOs in Improving Security Posture 7
What does the EAID Solution Offer? 9
How Can the EAID Solution Empower CISOs? 11
Conclusion 15

Introduction

Years into the digital revolution, digital information in all parts of the world is constantly subjected to unethical attempts at data manipulation, thefts, and unauthorized distribution. The cyber risk landscape is intense irrespective of the size, industry, or location of your business operations. How, then, is an organization supposed to safeguard its data?

All organizations require an efficient, robust, and actionable risk assessment, compliance, and remediation plan to protect their digital assets from malicious sections of the cybersphere. Most organizations employ Chief Information Security Officers (CISOs) to take care of these needs. As the CISO of your company, you are trusted with the enormous responsibilities of developing, monitoring, upgrading, and promoting your organization's information security policies. Many sub-tasks are included under each of these responsibilities.

A major sub-task under the development of information security policies is conducting risk assessments of multiple kinds such as information security, physical security, application security, third-party vendors, and compliance. Similarly, monitoring your organization's information security policies is not limited to the supervision of new potent cyber risks and the organization's security posture. It also includes checking if your employees are compliant with the security policies and if new changes have been made to any of the federal or state laws and industry standards that regulate your business operations.

Additionally, all information security policies require regular up-gradation based on a thorough analysis of your organization's new vulnerabilities as well as the new risks that are released into the cybersphere every minute. Based on risk and vulnerability analysis, compliance policies, as well as the remediation efforts in your organization, this all helps determine what needs to be upgraded.

Lastly, promoting your organization's information security policies is a crucial but often overlooked job that a CISO must perform. This requires that the information policies be designed and defined in a manner that is comprehensible to the employees who may not be experts in the areas of IT and information security. It is also a CISOs responsibility to ensure that regular reminders about your organization's security, compliance, and remediation policies are sent to the stakeholders within your organization as well as outside the organization in the form of third-party vendors or even your customers. Promoting also includes training your employees on the importance of data security and compliance. In the forthcoming sections of this book, we will describe these different responsibilities of CISOs in greater detail.

Since a CISOs responsibility is so critical to the business operations of an organization, the job can seem daunting to anyone. Moreover, after looking at the tasks that come under a CISOs purview, it is hopefully clear that a CISOs job is also very multi-faceted. So much so that streamlining the various tasks, some of which need to be conducted simultaneously and continually, can be extremely difficult. This is true not only for big corporations but also for smaller organizations.

If you are a new or even an experienced CISO, BizzSecure has developed a way to make your life simpler and your job far more efficient. BizzSecure's Enterprise Assessment and InfoSec Design

(EAID) solution has been empowering CISOs across organizations in a variety of fields including health, education, and finance among others. The EAID solution helps you streamline and integrate your operations of risk and compliance assessments, security policy design, remediation efforts, resource allocation, and audits.

Through this book, we hope to present to you the numerous ways in which the EAID solution can empower you as the CISO of your organization. We first delve deep into what it means to be the CISO of an organization and the variety of responsibilities that CISOs share. We follow this discussion with how BizzSecure's EAID solution is and can be changing the way CISOs operate. Finally, we provide insights into what jobs of a CISO can be eased by using the EAID solution, and how the software accomplishes that.

Who is a CISO?

Simply put, a Chief Information Security Officer (CISO) is a management position that leads, organizes and oversees all information and data security operations at an organization. As we have mentioned before, a CISO is tasked with a range of jobs including risk assessment, risk management, and remediation and consulting with law enforcement and regulatory bodies about the organization's security posture.

It is a high-level job and demands the honor, dedication, and experience of any other such high-level job. CISOs tend to have extensive experience and training as information security managers, analysts or engineers. Their training and expertise make them apt to perform a host of jobs. Let us take a look at some of the basic responsibilities of a CISO.

Creating a team of experts

The first thing a CISO must do is assemble an efficient team of IT and information security experts. It is the CISO's job to train and mentor this newly appointed team on all security matters concerning your organization's business operations. Experts from both IT and information security are required to drive an effective security campaign in any organization. Both these departments must work in tandem and use each other's expertise to design great information security policies. Integrating the two departments is also a job of the CISO. IT experts will typically work with software and maintain your organization's computer systems and servers. On the other hand, information security experts will focus on the organization's data security through calculated risk and vulnerability analyses, remediation planning and the use of IT resource to implement the organization's security plans. Therefore, in an integrated manner, the IT experts in a CISO's team would be involved in the development of IT systems to realize the information security policies designed by the information security experts.

Designing information security policies

One of the most vital jobs of a CISO is to design and develop information security policies. Depending on the size of your organization, the CISO could either supervise a team of relevant experts to design the policies or do it on their own. Information security policies must be designed to be customized to your organization's needs and vulnerabilities. This requires thorough risk assessments and vulnerability analyses using your organization's current security framework. If yours is a new organization, the CISO will need to perform these analyses and assessments from scratch. Based on the results of the assessments, the CISO should be able to come up with an actionable security policy for your organization.

Developing risk management plans

It is also a CISO's job to design risk management policies in collaboration with all the stakeholders in your organization. Sometimes, this may also include your clients or customers. Risk management incorporates risk remediation as well as risk mitigation. Remediation is performed when an incumbent threat can be eliminated at the roots with one or measures laid out in your policy. Mitigation is used when the threat can only be contained, not eliminated. Many a time,

both remediation and mitigation measures are used in tandem to reduce the harms caused by cyber threats.

Ensuring compliance with security policies

A CISO must understand the importance of compliance to both external regulatory policies and standards, and the organization's internal security management policies. It is any CISO's job to enforce compliance of these internal and external policies by all people in the organization – all employees working at any level with the organization's data assets. A CISO can make use of creative ways to enforce compliance. These can include easy, effective, and creative communication of your organization's security policies to the employees so that the recall ability of compliance and security policies is high.

Allocating resources for efficient security management

A CISO must also allocate the resources, both financial and human, required to successfully bring about a security operation in your organization. This has to be done in close collaboration with the finance department because they will communicate their budgetary constraints to the CISO. The finances must be balanced in that they should allow for continued security monitoring and up-gradation for policies in the future, while also effectively meeting the current requirements of information security. In case the information security budget needs to be increased, it is the CISO who will talk to the top-tier stakeholders in the organization and convince them to get the budget approved. Moreover, the CISO must also be able to do a forecast of the financial resources required for security policies and related operations in the future.

Conduct security and compliance audits

To ensure that your organization's security and compliance efforts are not lacking in any domain, the CISO must conduct or supervise frequent audits of information and application security, third-party vendors, and compliance within your organization. Such audits help detect any flaws in the current security framework of your organization. Internal audits by the CISO and their team also help your organization prepare for official audits conducted by regulatory authorities from the government and the industry.

Role of CISOs in Improving Security Posture

All assets or resources associated with digital information form a part of your 'data assets.' These include the software, the hardware, as well as the network used to generate, process or share your organization's data. The reason why so many organizations, irrespective of their size or business, appoint a CISO is that the security of an organization's data cannot be taken lightly. In fact, certain industry regulations make the appointment of a CISO mandatory. Clearly, information security is a necessary and burdensome task that requires a well-trained and experienced security officer.

Apart from the tasks listed in their usual job description, there are some unique tasks that CISOs can undertake to help improve and maintain the security posture of their organizations. Let us take a look at some of these tasks.

Conduct a real-time cyber threat analysis

In today's digital age, new cyber threats can generate as quickly as you create new data. If your organization obtains, stores, or shares any sensitive information pertaining to your employees and your customers, it can be a target of malicious cybercriminals. In this situation, it becomes necessary that CISOs engage in real-time cyber threat analysis to be on top of your organization's information security game. In addition, the CISO must also conduct real-time vulnerability analyses based on your organization's current information security policies and compliance track records.

Perform risk discovery and prediction

Since new cyber threats are developed so quickly in this age, it is important to be one step ahead of your malevolent opponents. Investing time and resources into discovering any imminent risks and predicting what future threats may look like is the only way to do this. Your organization's CISO and their team is well-equipped to perform this task. In addition, third-party vendors may be supplying you with applications and software crucial to your business operations. The CISO should also analyze and decide which of these new vendors or applications are trustworthy and secure enough to be used by your organization. Overall, being prepared for any new threats will help improve your organization's security posture.

Use cyber-forensics to understand security failures

There may be times when even with an excellent CISO and a well-oiled InfoSec team, your organization is exposed to a dangerous cyber threat. The hope is that you still have prompt remediation measures to contain the threat. Nevertheless, such a breach exposes some major vulnerabilities in your organization's security policies. In such cases, a CISO can appoint a cyber-forensics team to perform an in-depth analysis of the security breach and understand what it tells about the weaknesses in the organization's current security framework. Such analyses will only boost your organization's immunity against any future cyber threats.

Engender awareness of cybersecurity policies

Your employees can deeply impact your organization's information security based on their compliance levels. It is the responsibility of a CISO to engender awareness of your organization's cybersecurity policies among all your employees. This involves conducting training sessions to make sure that your employees, as well as the leadership in the organization, understand the security policies to the letter. This knowledge will ensure that they are more compliant with the policies and regulations. This will, in turn, improve your organization's security posture.

Communicate new developments in the cybersphere with top-tier personnel

A CISO also has the job of communicating the new developments in the areas of cyber risks as well as the ways to tackle them with your organization's top-tier staff such as C-level officers and the board of governors. A timely conversation with these stakeholders makes sure that sufficient resources are allocated for remediation planning as per the newly emerged cyber threats.

Understanding the ways to improve your organization's security posture through an efficient and reliable CISO could be highly beneficial for your business operations and its continuity.

What does the EAID Solution Offer?

We have now seen what CISOs do to improve your organization's security posture. To help CISOs in their humongous job, BizzSecure launched its EAID solution to aid your organization in securing its data and information in a better, automated, and more efficient manner. Organizations that use the EAID solution get the advantage of generating, visualizing, editing and updating all data security-related information and processes on a single portal. Several organizations in the fields of education, healthcare, retail, finance, manufacturing, energy, and government have found the EAID solution to be a valuable tool.

The EAID solution aims to eliminate your need to perform time-consuming and expensive manual assessments of risks, remediation, and compliance in your organization. The team behind the EAID solution has painstakingly designed over 1,800 policy templates so that the users of this software are able to develop their own risk management, compliance, and risk remediation policies.

The EAID solution is one platform for all the security needs that your organization has. Let us take a closer look at what the EAID solution can do.

It makes audits and risk assessments easy

Regular audits and risk assessments are vital for the success of any security operation. Performing audits and assessments manually can greatly decrease the efficiency of security operations in your organization. Moreover, maintaining the regularity of audits and risk assessments would mean allocating more person-days to these jobs. The EAID solution provides an efficacious answer to these problems. It provides a way to automate both IT and other security audits as well as risk assessments.

It helps enforce compliance with regulatory laws and standards

The EAID solution guides your organization on regulatory bodies and their compliance requirements. Users can select from over 12 different regulatory bodies and standards based on the kind of business operations they are running. Specifically, the EAID solution provides compliance support for several regulatory bodies and security frameworks which include HIPAA-HITECH, PCI-DSS, AICPA SOC2, NIST 800-53, NIST 800-171, NIST CSF, FFIEC, FISMA, ISO 27001, ISO 27002, GDPR, CCPA, FedRAMP, FISMA, SIG, the cyber security framework and others. Thus, no matter what industry you are in or what laws and standards regulate your organization, the EAID solution has got you covered.

It brings together your IT and Information Security departments

As we have discussed before, a CISO is tasked with the creation of a team of experts from the IT and information security departments. The EAID solution brings together these two departments in any organization by integrating their respective contributions to security operations into a single portal. The integration of these two departments saves time and resources invested in security operations.

It is a robust information security platform

As cyber threats evolve with time, it becomes important to make your security framework more robust for up-gradation and modification. The EAID solution makes your security policy design robust because it allows for an up-gradation of policies based on your risk assessments. Moreover, the EAID solution can be used across physical locations, vendors, organizational departments, and industries, which makes it a robust, one-stop platform for all your security requirements.

It reduces resource overhead

Any CISO would appreciate the financial and human resources invested in the various tasks that enforce and maintain the security framework of their organization. The resource overhead is particularly concerning when all the security management tasks are done manually. The EAID solution resolves this issue because all aspects of information security are automated and integrated through this platform. With minimal resources invested in security design, risk assessment, compliance, and risk remediation, your CISO's team will have more time, energy, and money to look over the security aspects that cannot be automated.

It stores all your risk and compliance assessment reports in one place

We have emphasized before the importance of the regularity and frequency of risk and compliance assessments in any organization. More frequent assessments eliminate complacency and improve preparedness against any incoming cyber threats. The EAID solution stores and maintains all the assessment reports collected over months, quarters, and years in your organization's various departments and geographical locations. A single place to store all the risk assessment information also improves the visibility of all risks in your organization. All concerned and authorized personnel can gain an insight into the risks that your organization faces by looking at these risk and compliance assessment reports. It also allows them to compare the reports from different times to monitor the improvements (or, perhaps in some cases, deterioration) in your security efforts.

It keeps a track of your remediation and mitigation efforts

Risk remediation and mitigation are the only ways to ward off a threat that has already penetrated your organization's security framework. The EAID solution helps you keep a track of all the remediation efforts that were either conducted in the past or are ongoing at this time. This increases the visibility of your remediation and mitigation efforts and helps you prioritize other risks depending on how far along your CISO and their team are in the risk remediation efforts.

Automation has become the keyword of the decade in the field of information security. BizzSecure's EAID solution helps you partially or fully automate each and every aspect of information security including risk assessment, policy design, compliance, security audits, and risk remediation. Looking at these features of the EAID solution, it can be expected that this platform can make a CISO's job more efficient in a lot of ways. In the upcoming section, we will provide a direct comparison of several jobs that a CISO performs and the ways in which the EAID solution can help make those tasks simpler and better for any CISO.

How Can the EAID Solution Empower CISOs?

As we have described in detail earlier in this book, CISOs have a massive responsibility towards their organization with a long list of jobs at hand. BizzSecure's EAID solution is designed to perform several tasks that are typically assigned to large IT and InfoSec teams. As mentioned before, these include assessing the current security risk landscape, ensuring compliance, enabling apt allocation of resources for security measures, devising remediation strategies, and many others.

Which of the CISO jobs that we have listed in the previous sections of this book can the EAID solution help to relieve and improve, and how? Let us take a look.

Quick assessment of the existing information security framework

What a CISO does: To come up with swift and relevant changes to security policies, a CISO and their team are required to perform a quick assessment of the information security system already in place in the organization. This allows for better strategic planning to safeguard the organization's data assets.

How the EAID solution helps: The EAID solution provides direct visibility into the current security framework of any organization, big or small. This automated solution empowers the CISOs with increased visibility of the security design, improved efficiency of their teams and reduced assessment time.

Efficient remediation of cyber-risks

What a CISO does: It is a CISO's job to devise effective remediation strategies for all the risks identified during assessments of information security, application security, third-party vendors and compliance.

How the EAID solution helps: The EAID solution helps assign specific remediation measures to each cybersecurity risk. It also links and integrates the different security risk assessments with remediation to help respond promptly in the event of a security disaster.

Keep track of different regulatory bodies and standards

What a CISO does: Many businesses are regulated by any number of federal or state laws and industry standards. These could be HIPAA-HITECH, SIG, ISO, PCI-DSS, NIST 800-53 or any of the several others. A CISO is also tasked with understanding the requirements of each regulatory body and checking if the organization has the resources and the framework to ensure compliance with that body.

How the EAID solution helps: The EAID portal assimilates over 12 different regulatory compliances in a single software portal to ease the CISO's task of tracking each and every relevant regulatory compliance policy. The CISO can select the regulatory policies that govern their organization's business operations and automatically compare the organization's current security framework to the requirements of the regulatory bodies.

Design information security policies

What a CISO does: This is one of the most important tasks a CISO must perform. The entire organization's data security relies on how well the information security policies are designed. Moreover, as cyber-threats evolve every hour, it becomes important for a CISO to keep up with new developments and update its organization's information security policies accordingly.

How the EAID solution helps: The EAID solution lets you design your own security policies by following one of the 1,800 different policy templates that the experts at BizzSecure have compiled for you. You can also custom design your own policy without using a previously available template. Various policies are also designed based on different kinds of compliance standards expected from organizations.

Easy job assignment

What a CISO does: Delegation is an important responsibility of any CISO. They must hire individuals with qualities and prior experience that resonates with the vast variety of steps required in information security management. When done manually, tasks such as security risk assessment, compliance assessment, risk remediation, and risk reassessment are assigned to members of the CISO's team.

How the EAID solution helps: The EAID solution helps assign review and assessment jobs to the different members of the CISO's team. It allows you to add users authorized to participate in assessments or reviews of already finished assessments and policies to the EAID portal. The assignees can perform assessments and reviews by logging into the EAID platform.

Collaboration with senior officials in the organization

What a CISO does: The CISO must also collaborate with the senior officials including other C-level officers and the board of governors to ensure proper review of the security policies designed by their information security and IT teams.

How the EAID solution helps: The EAID solution provides clear visibility to the risks and benefits of the security policies of your organization. Reports and assessments can be generated and shared promptly with all the high-level stakeholders in your organization. They can even provide feedback by answering specific questionnaires on the EAID platform.

Conducting risk assessments

What a CISO does: Risk assessment is the first step when designing an information security policy. Your organization's CISO must be adept at achieving thorough risk assessments for information security, physical security, application security, third-party vendors, and compliance.

How the EAID solution helps: The EAID solution provides a way to conduct all kinds of risk assessments in an automated fashion. Experienced experts at BizzSecure have put together over 9,300 questions that authorized users can answer on the platform as part of risk assessments. The

questions pertain to information security, application security, vendor risks, physical locations, and compliance. The EAID platform also requires the users performing these assessments to provide relevant pieces of evidence to validate their responses.

Generating and sharing risk assessment reports

What a CISO does: We have mentioned before that performing risk assessment is an important job of a CISO. It is also important to communicate the results of these assessments with the stakeholders in your organization. That responsibility also lies with the CISO and their team. They must generate quick and easily understandable risk assessment reports and share them with the employees and leadership in your organization.

How the EAID solution helps: The EAID solution is equipped with a 'risk report dashboard' where you and other authorized users can look at the results of any risk assessment pertaining to your organization. This dashboard greatly improves the visibility of risk assessments for all the personnel authorized to review risk assessment reports. The EAID solution also makes it simple to generate and export risk assessment reports and then share them with other concerned parties promptly.

Weighing and prioritizing security and compliance risks

What a CISO does: We have previously discussed how important it is for a CISO to ensure proper allocation of financial and human resources for risk and security management. A proper allocation strategy is to weigh the risks that your organization faces based on vulnerability analysis. Weighing the risks helps the CISO assign priorities to the risks for resource allocation and risk remediation.

How the EAID solution helps: The EAID solution lets you assign each cyber risk (identified through prior risk assessments) a weight depending on the extent of the threat posed by that risk. This way, all risks will get classified into different risk levels – 'low risk,' 'medium risk,' 'high risk,' or 'critical risk'. This classification makes it easier for everyone to understand the proportion of risks that are likely to turn into live threats. It also helps identify the risks that should be prioritized for subsequent resource allocation to conduct risk remediation and mitigation efforts.

Increasing resource visibility

What a CISO does: Another important aspect of ensuring appropriate resource allocation for security efforts is to know exactly what resources you have and can allocate. This aspect is closely knit with several other people or departments in your organization that help defines the budget allocation during any financial year. The CISO performs a financial forecast for its department to ensure that the security efforts get the money they deserve.

How the EAID solution helps: The EAID solution improves the visibility of resources in your organization. The CISO can keep an eye on what resources are at their disposal at any given time. Based on the risk assessment and classification, the CISO can decide which risks require more resources for remediation. The EAID solution also gives the CISO a look into previous years' resource allocation and strategies. This will help the CISO formulate a better allocation plan for the current year.

Tracking the progress of risk remediation and risk mitigation

What a CISO does: A CISO must keep constant records of how any ongoing risk remediation and mitigation tasks in the organization are progressing. This allows them to reassess the risks that are not properly remediated or mitigated. Based on the progress of risk remediation and mitigation efforts, the CISO may also decide to change the resource allocation for risk management.

How the EAID solution helps: The EAID solution helps CISOs by keeping a continual and real-time track of all risk remediation and mitigation efforts in their organizations. Moreover, it provides a robust way to conduct a reassessment of risks based on remediation efforts. The EAID solution performs risk reassessment by asking authorized users to answer the same questionnaire that they answered during the risk assessment. However, this time, the users are supposed to consider the remediation and mitigation efforts and provide evidence accordingly.

Monitoring the maturity of your security framework

What a CISO does: A behind-the-scenes task for all CISOs is to compare the health of their organizations' current security frameworks with the records from the previous years. This helps the CISOs track how their security framework has matured over the years. This can be a cumbersome task for the CISO requiring security visibility, tracking of the organization's security posture and comparative analyses.

How the EAID solution helps: The EAID solution automatically lets CISOs track the maturity of their organization's security frameworks. Since all your security efforts from over the years are compiled together on a single platform, it enhances the visibility of the health of your organization's security system. Improved visibility makes it easier to compare how your security has tracked over time.

Looking at the numerous points discussed above, BizzSecure's EAID solution provides direct relief to CISOs on a lot of fronts. It empowers them by effectively helping in the design, maintenance, and up-gradation of your organization's information security system.

Conclusion

Whether or not your industry requires your organization to appoint a CISO, you should go ahead and start looking for one. CISOs are tasked to do a lot of jobs in order to cultivate and maintain your organization's information security framework. Given the breadth and depth of a CISO's job, a CISO cannot ever be completely replaced with a software portal. However, the EAID solution is an intelligent, integrated software platform that seeks to empower all CISOs by helping them perform their countless jobs in a much better and more streamlined way. It saves them time, resources and energy so they can focus their attention on the security tasks that cannot simply be taken over by software.

One of the aims of this book was to make you familiar with the concept and functions of a CISO in any organization. We have also paid special emphasis on how BizzSecure's EAID solution can be used to make a CISO's job better, easier, and more efficient.

We hope that through the first few sections of the book, we were able to help you realize how important and indispensable the job of a CISO is to an organization's security posture and business continuity. After covering CISO basics, we comprehensively discussed what the EAID solution brings to the table for any organization. Finally, we provided a one to one correlation and comparison between various jobs that come under the purview of a CISO and how the EAID solution improves and relieves these jobs to makes a CISO's task easier, greatly empowering them in the process.

Hopefully, we have encouraged you to get a subscription to BizzSecure's all-in-one answer to all your organization's security-related problems – the EAID solution. Use the EAID solution and empower your organization's CISO today.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com