BizzSecure
PEACE OF MIND FOR InfoSec

Top Five Challenges for CISOs

Table of Contents

Introduction 3

Who Is The CISO? 5

What Does the CISO Do? 6

Skills Required of A CISO 8

Top Five Challenges for CISOs Unveiled 11

Final Words 16

Introduction

Information is power.

At least, that’s what has been proven in the 21st century. With organizations leaning heavily on digital systems for carrying out their daily operations, it’s no wonder that we are generating more data and information.

At least in the short term.

As a result, the need to store this information securely, and ensuring the continued safeguarding of thsuch data has become a matter of paramount concern. Businesses are literally losing money from data leaks and information misuse. Therefore, it’s natural that they want to create a system where the entire data infrastructure remains safe and can preserve its integrity.

This is where the Chief Information Security Officer (CISO) comes in.

The CISO is a relatively new position in the corporate hierarchy (they’ve been around for about 25 years) but has already succeeded in occupying a position of immense importance. While most organizations already have a CISO in place, some businesses have yet to define and fill this most important office. This is a serious loophole that can result in disastrous outcomes for your business.

The current information security landscape is extremely complex and ever-evolving, to say the least. As threats continue to morph and change by the moment, attackers are quick to adapt and develop new modes of gaining entry into your business’s information systems. Today’s complicated threat landscape has begun to disrupt existing business functions, therefore, the role of the CISO is becoming more and more relevant.

With the scope of the CISO’s responsibilities and duties growing larger by the minute, CISOs are coming to the forefront of company operations in greater prominence than ever before. Currently, cybersecurity is viewed as one of the most critical aspects that influence an organization’s bottom line, and CISOs are interfacing more closely with other C-suite executives to ensure the continued safety of business data.

The job of the CISO is easier described than carried out. The task of the CISO primarily involves the management of cybersecurity threats, but this task is complicated by several factors such as an increasingly expanding attack surface, and security complications arising from the expansion of networks. Add to that the disruption introduced by the latest technological innovations such as AI and IoT, and the task seems utterly impossible.

CISOs can no longer be content with just focusing on the information technology side of things. They must also take an active part in the daily development of a business strategy. It’s imperative that CISOs make the move from being mere compliance followers to taking a broad-based approach to the organization’s overall risk management strategy.

In order to do so, however, CISOs must overcome several hurdles on the path to success. In this eBook, we are going to take a close look at the top five challenges that CISOs must face in the line of duty. Along with that, we are also going to grab sneak peek at the most important responsibilities of a CISO, along with the qualities that are expected from a professional holding the designation.

So as usual, let us begin at the very beginning, and start off our discussion with the most basic question of all: who is a CISO?

Who Is The CISO?

We want to leave no stones unturned in our discussion, therefore, we have decided to start the topic with formally defining who the CISO is. Put simply, the CISO is an executive responsible for looking after an organization's data as well as information security. Till in the recent past, the job of the CISO has been largely confined to technological spheres alone. Now, however, CISOs are seen to take up more expansive roles and responsibilities.

It's part of the CISO's job description to formulate, establish, and maintain the vision of the enterprise regarding data protection. The CISO is responsible for directing staff in order to identify, develop, implement, and maintain processes across the organization that result in a significant reduction of the risks that might be posed to the IT assets of the company.

A CISO is a person who responds to any form of IT threat to the organization; they are also charged with the task of establishing the appropriate standards and controls regarding information security practices in the organization. They also have to take special cognizance of any compliance-related issues that the business may be facing.

A CISO or equivalent designation-holder has become a standard role in major as well as small business operations, governments, and even educational and non-profit organizations. Apart from cybersecurity issues, the role of the CISO has evolved to encompass handling risks inherent in business processes, customer privacy issues, and other critical business functions.

Due to the broadening role of the CISO, they are no longer constrained to being functionaries of the IT department. At present, only a handful of CISOs actually reports to the CIO (Chief Information Officer); most usually report directly to the board of directors or the CEO. This has resulted in the CISO function becoming delinked from that of the CIO. In fact, such an arrangement is considered the optimal one as the responsibilities of the CISO extend far beyond that of the IT department.

In general, CISOs need to possess a nuanced balance between business acumen and technological know-how. With high salaries and the prospect of brilliant career growth, the CISO position has become one of the most coveted ones in the corporate hierarchy.

Now that we know all about who and what the CISO is, let's take a detailed look at some of the many responsibilities that a CISO is expected to fulfill.

What Does the CISO Do?

In the previous section, while defining what a CISO is, we've already taken a cursory glance at the responsibilities of a CISO. However, the role of the CISO involves complex intra- as well as inter-organizational functions that warrant a separate discussion.

Therefore, in this section, we are going to explore the many responsibilities of a CISO and gain an understanding of what it is that they actually do or are expected to do.

Let's begin.

First and foremost, the CISO is responsible for handling all the information security operations of the organization. This includes conducting real-time analysis of threats that might put the company infrastructure in danger, such as firewall breaches, entry point monitoring, and database management. Also, when something does go wrong, the responsibility of performing triage falls with the CISO. This is of vital importance in order to assess the degree of damage done, and how to prioritize and handle the situation.

Secondly, the task of the CISO involves keeping tabs on any or all threats that are developing or have developed to put the company infrastructure in danger. In the case of mergers, acquisitions or similar business moves, the CISO is responsible for keeping the potential security problems from becoming a reality. CISOs often directly interface with the board of directors in order to keep ahead of the security curve. They may also have to handle the responsibility of quantifying the impact of a cyber-threat and measuring the financial implications of the the threat.

The next responsibility that the CISO must shoulder is that of ensuring the prevention of fraud and loss of data. Most often, greater threats to an organization come from the inside than the outside. This typically involves employees compromising sensitive information, the intentional or unintentional destruction or leakage of critical business data, or the leak of intellectual property-related data. CISOs are responsible for making sure that such situations do not arise by monitoring information flow within and between organizations and noticing any abnormal data spike that may occur.

Looking after the security architecture of the organization also falls under the umbrella of the CISO. It is the CISO who is responsible for building the security structure of the organization, such as creating an adequate firewall system. CISOs may also take decisions regarding the network segmentation and architecture of the computer systems in use in the organization. In order to test out the defenses, CISOs usually rely on ethical hackers and pen testers to sample the defenses in place. Lack of proper network security architecture can result in so-called "flat" networks; here the malware that infects a single node can quickly spread across the entire architecture and cause severe damage. A well-segmented network is sure to have proper safeguards in place so as to be able to segregate and isolate infected portions, thus protecting the rest of the infrastructure. In short, it's the CISO who makes sure that the network infrastructure is designed with the best security practices in mind.

The next important activity that the CISO must undertake is access management. In any business, an employee has to handle several sensitive business documents with critical information. In the age of digital, these can only too easily be whisked away. The CISO is the person who must ensure that every employee has access to what they need, and only what they need. Also, the moment an employee ceases to occupy a particular role, it’s the CISO’s responsibility to ensure that the person no longer has access to company data. Otherwise, this may lead to severe information leakage.

It’s the CISO who must layout and manage all information security programs that need to be implemented across the organization. The CISO needs to measure the present as well as probable risks, gather intelligence, map data paths and identify gaps where applicable. One common example of a CISO’s daily routine would be to assess all security patches and apply them on a regular basis. Patchy patchwork (pun intended) can lead to massive data disasters.

Last, but certainly not the least, it’s the CISO who is responsible for leading the charge of all forensic investigations. CISOs have to be pros in cybersecurity and need to have a thorough knowledge of all cybersecurity-related laws and procedures.

In the case of an incident, CISOs need to work with external law enforcement agencies and consulting firms in order to conduct detailed cyber-forensic investigations of the breach. Often, they may embark upon the task on their own. CISOs are also the people who look into errant employee behavior and take steps against the perpetrators.

It can easily be said that the CISO spearheads the security efforts of any organization. This rather critical position cannot be filled by just anyone. A CISO has to be a person who can adequately combine domain knowledge and industry expertise with the required coordination and investigation skills that are essential to guarantee that the role is carried out perfectly. What exactly are the requirements for a top-notch CISO?

That’s exactly what we are about to explore next.

Skills Required of A CISO

Gone are the days when the main responsibilities of the CISO used to be password management and firewall maintenance. Today, the role of the CISO has expanded to include leadership responsibilities specific to the business. The CISO of today is regarded as one of the most essential members of the executive team and is no longer restricted to the technical domain alone.

Thus, the role of the CISO is now more demanding than it ever was before, and with good reason. Unless the CISO can successfully interface with the multiple departments and move across industry verticals with ease, then the functioning of the job itself becomes faulty. With that in mind, let’s take a look at the essential skills a CISO must possess to fulfill their duties responsibly and effectively.

A Combination of Tech and Business Sense

It’s not necessary that CISOs have to come from technical backgrounds. In fact, the typical CISO often holds business qualifications such as an MBA in finance. A degree in computer science or related fields can certainly give the incumbent an added advantage.

In fact, if you think closely about it, both play an equally important role. While technical skills allow the candidate to navigate the rapidly changing technical sphere with ease, business skills allow them to effectively communicate with the rest of the C-suite and carry out the required operations.

Sound Planning and Management Skills

A CISO should have strategic planning as well as management skills which allow them to engage assistance across all levels of the organization and garner strong support. Primarily, the CISO needs to work with the company executives and ensure that the information security plans are in line with the company objectives and intended risk policy.

Other than the above, the CISO needs to have a clear sense of all technological and information related projects that are currently being undertaken by the organization. By doing this, the CISO can make sure that the information security parameters are integrated into every project at every step of the development.

Finally, the CISO should be an observant personality, who can spot industry trends and scan the threat landscape to protect the organization from emerging dangers.

Clear Communication Capability

Communication skills are essential to the functioning of a CISO; at any instance of time, the CISO must be aware of their audience’s level of expertise and modulate their communication channels accordingly. For example, when dealing with C-suite executives, the CISO must be able to elucidate security problems in terms of business so that it resonates with the top-level management. At the same time, they must also be capable of explaining the required security principles to lower-level employees as well.

Policy Development and Implementation Skills

A CISO needs to be an expert policy developer, but his skills must not stop there alone. Policies that are formulated and then rot in files are actually useless. A well-performing CISO must be capable of ensuring that the security policies are aligned according to the organizational goals and meet the requirements of the business.

Further, the CISO should also have enough adeptness to guarantee that the policies that are formulated, get implemented across all levels of the company. To do this, the policies formulated must be implementable by the organization and secure the work environment. Above all, they must meet the legal and regulatory standards that the business is expected to follow.

Political Navigability

The job of the CISO requires interdepartmental navigability. Therefore, the CISO must be adept at picking up the different political undertones that resonate across the business. This is critical to ensuring the success of the information security program.

The CISO needs to be capable of understanding the requirements of the executives, and also of presenting the InfoSec program as the potential solution to their needs. This way, they are sure to gain the support of top-level management.

For those in the lower rungs of the corporate hierarchy, the CISO should communicate the sense that security policies are meant to make their jobs easier and safer. It’s the job of the CISO to guarantee that the security measures are not seen as hindrances but rather as enabling factors.

Achieving the above successfully requires a large amount of political understanding of the organizational landscape.

Ability to Manage Conflict

There used to be a time when the role of the CISO was confined to handling the nitty-gritty of the IT department. Now, the CISO is required to actively participate with multiple stakeholders across the organization in order to carry out their functions effectively.

The CISO of today works with multiple teams on issues that actively influence the operation of the organization. It’s the job of the CISO to take care of conflicts, ensure that security needs are looked after effectively, and offer the guidance required to resolve conflicts smoothly.

The job of the CISO does not end within the company itself; they also need to work with the end-consumers and deliver the right training that facilitates the adoption of information technology best practices.

Financial Expertise

In the business world, the bottom-line matters; ROI drives decisions in the boardrooms, and unless the CISOs can effectively articulate the cost benefits of implementing new security practices, they are not going get the clearance to carry them out.

Therefore, the CISO must be able to fully explain the ROI for any and all security solutions that need to be implemented. Successfully communicating the rewards for investment to upper management, and that too in business terms that appeal to them, will not only allow CISOs to get the initial buy-in but also enable them to communicate the importance of the same throughout the organization.

Ability to Supervise Effectively

In the complex cybersecurity landscape of the 21st century, the role of the CISO is no longer limited to a single person. Instead, the professional in charge of the role must be able to take along with them an able team that can get the job done.

Therefore, it is of vital importance that the CISOs are able to interface properly with their teams and mentor them effectively to get the job done. When the CISO works with the team to develop their skill sets, it leads to a more engaged workforce, better communication, and at the end a more effective security regime.

Knowledge of Regulatory Standards

Finally, the CISO needs to be well-versed with the standards and regulatory compliances that are applicable to the business at hand. By doing this, the CISO can effectively focus on the individual needs of the organization, usher in the development of relevant security policies, and put in place processes and procedures that get the job done.

The above skills, coupled with sound professionalism, can lead to a better functioning organization in terms of security. However, the task of the CISO is made more complicated by the ever-morphing attack surfaces that organizations are exposed against. In the line of duty, the CISO has to face numerous challenges and difficulties.

These make the job of the CISO all the more critical, and this very topic is the point of our next and most vital discussion. In this, we are going to take a look at the top 5 challenges that CISOs face during work; we are also going to discuss some ways of overcoming these as well.

Top Five Challenges for CISOs Unveiled

We've spent considerable time discussing the various aspects of the CISO role till now. Essentially, all of the above has been the groundwork for what comes next. We already know that the CISO of today must be equally adept in the server room as well as the boardrooms. They must be agile leaders, an expert communicator, and possess the perfect blend of tech know-how with business acumen.

While this makes the role of the CISO definitely exciting, it's also more difficult. With the scope of the CISO role constantly changing, along with an increasing spate of cybersecurity incidents, the CISO needs to protect the organization from both insides as well as outside dangers. Add to that complex regulatory requirements, and you've got a combination that's more complicated than spaghetti.

As a result, CISOs the world over are facing multiple challenges and difficulties. These challenges not only stand as impediments to the path of on-the-job success but also affect the personal life and health of the CISOs negatively. Hence, it's very important to understand what these are and how we can tackle them.

Listed below are the five most challenging issues for CISOs in current times. Note, however, that this is not an exhaustive list. With the cybersecurity world undergoing significant changes every moment, challenges are taking on new shapes too. Here we'll try to capture the essence of the most important problems that CISOs have to face.

So here it goes:

Constantly Keeping Up To Date

One of the most challenging aspects of the job of a CISO is keeping up with the lighting fast change that takes place across the cybersecurity landscape every moment. With organizations racing to stay ahead of the curve, competition is stiff for cyber supremacy.

In such a situation, the job of the CISO is never really completed. Rapid advances in technology, especially IoT and AI, have created new attack surfaces that the CISO must consider as well. As disruptive technologies continue to connect people as well as things in more ubiquitous ways, the job of the CISO becomes infinitely more challenging.

CISOs must be up to date with the most important technological advances of the times, both in terms of hardware and software. Not only must they take the time and make the effort to apply the latest software patches that are relevant to maintaining the security of the organizational infrastructure but also they must have a full inventory of all hardware resources being used across the organization, the software solutions that have been deployed, and also keep track of which employees have access to which resources.

For large organizations, doing all this successfully can become a significant challenge. Maintaining cybersecurity and keeping on top of technological advancements is one of the greatest challenges that CISOs face. In order to overcome this, CISOs must work with a vigilant team and be ready to retrain and update themselves at every turn.

The Ever-Changing Tech-Landscape

Closely related to keeping up to date, the present technology landscape has empowered as well as encumbered CISOs to a large extent. While the plethoras of tech solutions lend themselves to placing a large number of resources at the hands of the CISOs, they have also had a negative impact.

The disruptive technological landscape of today, in spite of being enabling, has contributed towards creating a thinly spread attack surface. This leads to the creation of numerous opportunities for malicious parties to find ways of attacking your business. While organizations are quick to adapt technological advancements in order to stay ahead of the business curve, they seldom if ever take the care to ensure that all aspects of security are completely addressed.

In light of the above, let us discuss some specific technological evolutions that have created a nebulous situation for CISOs.

First off, let’s handle the Cloud. The cloud is one of the most important tech-innovations of the present times. As companies scramble to take their IT operations cloud-wards, the security of the cloud must dominate the agenda of the CISOs.

With a large number of companies moving their applications to the cloud, companies are hopeful of taking advantage of the flexibility, manageability, and scalability that this technology offers. At the same time, organizations remain hesitant due to the technological complexities that are inherent in the process. Until today, there aren’t many professionals who are well adept in all aspects of the cloud. This is something that the first movers witness when they try to take the step forward.

CISOs are the professionals who are most concerned with operations being moved to the cloud. By definition, the cloud is a loosely defined structure that is inherently insecure. This creates an indefinite attack surface that can be breached from multiple locations. The cloud is one of the biggest challenges that CISOs must face while ensuring organizational data and information security.

Another complex technology that is doing the rounds is AI, which is perhaps more nebulous than the cloud. Artificial Intelligence is still in a gray area and how it will impact the information security scene is not really very clear yet. As businesses move to incorporate AI and automation in their everyday operations, CISOs must remain extra vigilant in order to ensure the safety of business information.

The final technology that we'd like to discuss is IoT. The Internet-of-Things is becoming ever-pervasive, and more and more ubiquitous devices are exchanging data among themselves. This data usually travels through wireless channels, thus creating a highly vulnerable attack surface that perpetrators may seek to exploit. CISOs dealing with IoT systems at the workplace must be ready to deploy ever-vigilant processes that can ensure the complete security of organizational data.

The above were only a few examples of the complex technological disruptions that the world is facing today. CISOs need to be constantly on the lookout to guarantee that the tech never overtakes them.

Finding, Training and Retaining The Right Talent

No matter how efficient the CISO is, information security cannot be a one-man show. And this is all the more true for organizations of a scope that deploy a large number of IT assets. This creates a demand for highly skilled professionals who can tackle complex InfoSec problems.

But here the supply lags far behind the demand. With technological innovations outstripping the human ability to adopt and adapt to them, the talent pool is becoming ever smaller and smaller. Without the right talent to take care of the organizational information structure, CISOs can feel at a loss.

Perhaps more important than finding the right talent is training and retaining that talent to work for the company. As not many people are aware of the skills required to handle InfoSec positions, finding and preparing the right personnel should be a top priority for CISOs all over the world. Mentoring is one of the most crucial aspects of creating a great InfoSec workforce; unless the CISO can act as a mentor to the team, they are bound to fall short of the requirements that are needed to get the job done.

Finally, CISOs need to make sure that the workforce is engaged and involved enough in the work of the organization. After all, there's nothing better than an engaged workforce for creating an environment of data security. However, the trouble is, most employees often view the InfoSec measures taken by CISOs as hindrances to daily work processes. Hence it is part of the CISOs' job description to educate the employees as well as the IT team in the nuances of data security. Once the employees have a clear idea regarding why InfoSec measures are important, they are sure to be more diligent in following through.

Further, keeping the workforce engaged in the task is essential to retaining them in the organization. Good talent is hard to come by, and CISOs need to be extra vigilant and ensure that high-performing employees don't fall prey to attrition. CISOs need to nurture a strong team that can work in unison with the rest of the organization. The path to achieving this lies in laying the focus on employer branding and constantly motivating the staff to keep performing.

Also important are, looking internally in the organization, finding and re-training the right talent. The best solution is to work with external experts who can bring the requisite expertise to the table as and when required.

Hierarchical Hindrances

For most businesses, information security is the top priority. At least, that's the way it should be. A major portion of the global CEOs loses sleep over the fact that cyber threats will negatively affect the organization's growth prospects.

Surprisingly, when CISOs actually try to implement cybersecurity measures, they often find that the requisite support from top management is lacking. When tough investment decisions or fast resolution are required, the delay made by the decision-makers can often throw attempts at improvement off the rails.

The reason for this is that most boards do not have the required technological expertise to provide adequate support to the CISOs in times of need. By lacking the knowhow to act as strategic partners with the CISOs, company top management may often pose more of a roadblock than enablement.

In fact, it is estimated that only 21% of boards admit that they can provide full support to the CISO in times of need. This is a drastically low number that must be increased immediately. Without support from the boards, CISOs cannot hope to function with complete efficiency. As the boardroom expertise in understanding the multifarious threats that the organization faces improves, so does the support CISOs get from the top management. This not only enables CISOs to work better but also lends to increasing the efficacy of cybersecurity efforts.

Further, the way the CISO is positioned in the organizational hierarchy can greatly determine their ability to garner the required influence and organizational visibility required to effectively tackle cybersecurity and InfoSec risks. When InfoSec is placed in organizational isolation at the level of operation or the C-suite, then it becomes tough to create a well-rounded understanding of InfoSec's influence on business risk.

In case the role of the CISO is entrenched in the IT department, then the task of the CISO becomes all the more difficult. As explained previously, the current role of the CISO expands far beyond mere IT functions and restricting the role to merely technological frontiers can actually do more harm than good.

Therefore, CISOs need to be accorded a place of prime importance in the organizational hierarchy and need to be given full support from the board. By doing so, companies can ensure that cybersecurity efforts remain on the point, and the CISO is able to function to full capacity.

Changing Regulations

Last, but certainly of prime import are changing regulations and compliance rules. Businesses need to make sure that they fulfill all the latest regulatory requirements that pertain to their organization. In order to do so, the CISO must become an expert in the appropriate rules and regulations.

However, the ever-changing nature of regulatory frameworks makes this difficult for CISOs to achieve. Therefore, they must pay special attention and ensure that they are aware of all compliance rules. If possible, it’s best to seek external help in this regard.

Final Words

This has been a long discussion, and so we are going to keep the conclusion short. We hope that by now, you have a clear understanding of the various challenges that a CISO has to face in their daily operation.

The role of the CISO has morphed greatly over the years, and we can only expect it to take newer forms as time passes. But with company cooperation, employee support and the right external help, CISOs can hope to carry out their duties with greater efficacy.

Until next time, we leave you hoping for a brighter cybersecurity landscape.

BizzSecure

PEACE OF MIND FOR InfoSec

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com