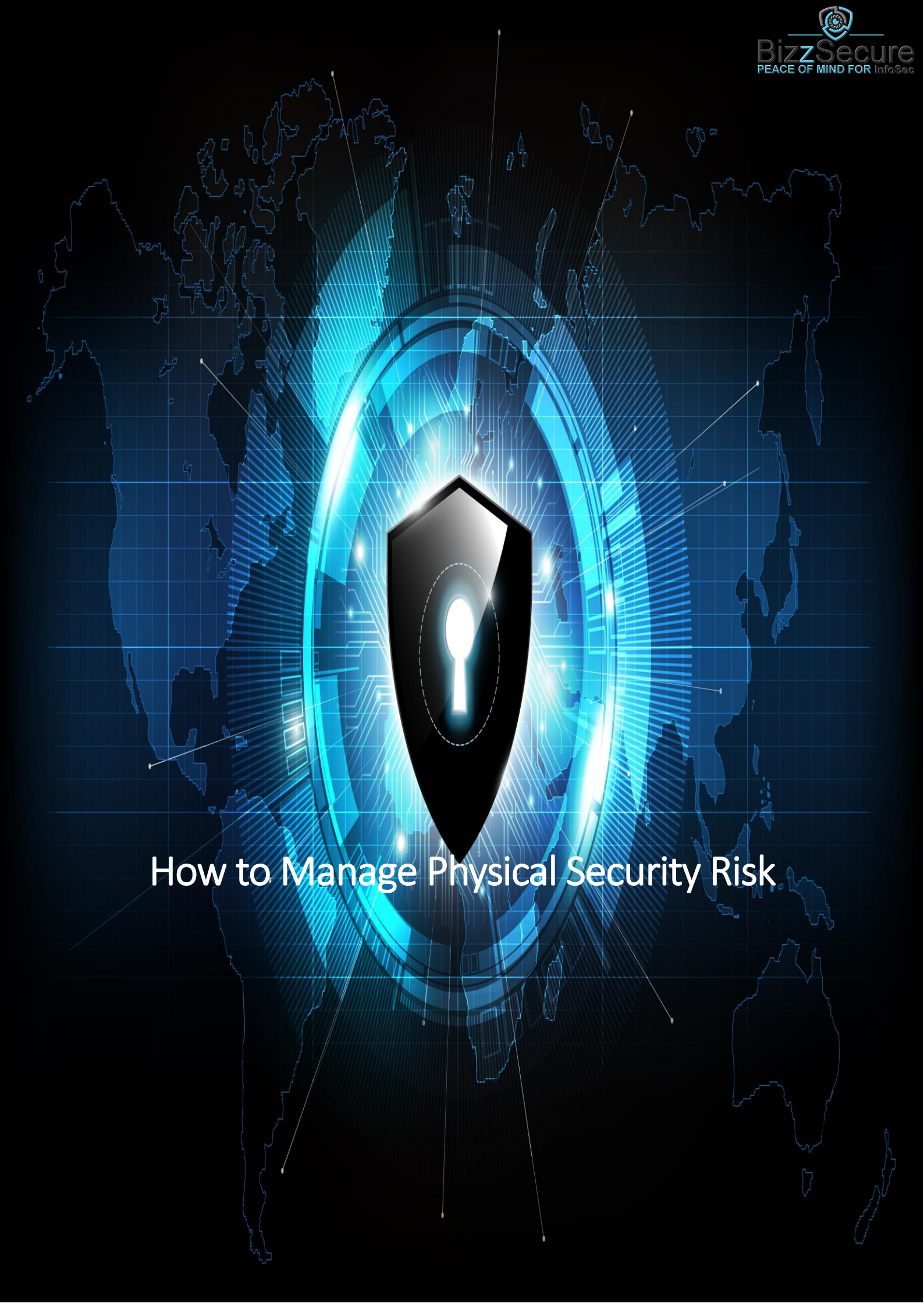
BizzSecure
PEACE OF MIND FOR InfoSec



How to Manage Physical Security Risk

Table of Contents

Introduction

Digital security has become the watchword of the day.

As we step into the new decade, the world is visibly dependent on IT infrastructure for carrying out everyday business operations. Be it monetary transactions or information exchange, digital platforms today dominate the world stage.

Naturally, digital data has taken the center stage in the grand scheme of things: with more and more devices coming online due to the advent of technologies such as wearables and IoT, this volume of data is only going to increase.Due to the rather sensitive nature of digital infrastructure, businesses are investing heavily in ensuring the digital security of their IT assets, and with newer, more sophisticated threats on the horizon, this is only to be expected.

Malicious elements on the internet are regularly amping up their repertoire of attack techniques. Ransomware, DDoS, and spyware are just some of the many weapons in the arsenal of these malicious players. In order to protect IT resources from such attacks, companies are prepared to invest time as well as money.

But are our present security measures enough?

True, you can put in place advanced digital security structures, create digital safety and hygiene protocols, and deploy state-of-the-art technology to ensure that your assets are *digitally* protected. All this overlooks one of the main chinks in the cybersecurity armor: physical security.

Consider this: you have implemented all the encryption in the world; you've created a digitally insulated system that cannot be penetrated by digital means. What if a fire happens to ravage your data servers? Or any unauthorized personnel gains access to secure areas of your computing infrastructure? What happens next?

Physical security was, is, and will remain one of the prime avenues by which your cyber-infrastructures can and should be adequately protected. Ensuring that your computer systems are well-guarded from unauthorized access should be paramount on the list of measures you plan to implement for guaranteeing the safety of your IT assets.

Keeping your organization safe against physical attacks is essential to safeguarding your digital assets. This not only helps to reduce the risks to your IT infrastructure but also contributes towards protecting your employees as well as related physical property.

Yet physical security rarely occupies a position of concern in the minds of most information security professionals. Seeing as physical security has multiple technical as well as administrative components, organizations fail to recognize it as a valid component of cybersecurity.

Physical security must be one of the key components of your digital security plan. Without a well laid physical security infrastructure, your digital security remains half-baked at best, and dangerously exposed at worst.

In our previous offerings, we have talked at length about multiple facets of digital security. Today, however, we are going to take a look at physical security measures, which is perhaps the most important link in the cybersecurity chain.

True to our tradition at BizzSecure, we assume nothing and begin at the very beginning. We start by laying out the definition of physical security in unambiguous terms; then we go on to explore the importance of physical security in the digital ecosystem. We are also going to take a close look at some common physical security protocols and define some specific types of physical security threats.

Finally, we will round off our discussion by enumerating a few best practices for planning and managing physical security, along with some handy tips that you can put into practice at your workplace.

We do have a lot to cover, don't we! So let's not delay further and start off with the first section of our concern.

What Is Physical Security Exactly?

In the plainest of terms, physical security can be defined as protecting organizational assets such as people, property, systems, and IT infrastructure from coming to harm as a result of physical events.

What are these physical events?

Physical events can span happenings such as fires, floods, natural disasters, and even crimes that are perpetrated against your company infrastructure. Yes, accidents also fall under the umbrella of physical events. A coffee cup spilling over your office laptop is as much a security risk as that hacker lurking in cyberspace.

Physical Security covers the safeguarding of personnel, hardware and software assets, network infrastructure, and digital data from physical events that can cause insidious loss or damage to a business, organization, or institution. As mentioned above, both man-made and natural disasters fall under the scope of physical security.

It is indeed a sad truth that physical security is seldom given the importance it deserves; it is most commonly overlooked in favor of technical safeguards involving cyberattacks and malware.

Now that we know what physical security risks comprise, we can take a closer look at the components of physical security.

Components of Physical Security

Primarily, physical security measures have three parts: Access Control, Surveillance, and Recovery Testing. Let us look at each of these components in turn.

Access Control

Access control is the first point of safety that physical security provides; it primarily consists of physical obstacles that must be placed in the path of potential threats. Important locations such as data centers and server farms should be well-fortified against any attacks, accidental mishaps, or natural disasters.

Fortification measures can include physical locks, fences, and access control mechanisms such as access cards, biometric identification systems, and security personnel.

Surveillance

It is commonly said that constant vigilance is the price of safety, and for physical security, this is truer than ever. In order to ensure the physical protection of your IT infrastructure and business premises, you need to guarantee that every part of your organization is actively monitored at all times.

Technological innovations such as CCTV systems, anti-intrusion sensors, and detection capabilities such as smoke detectors can help in this regard. Ensuring the continued surveillance of your IT assets is paramount to safeguarding them.

Recovery Testing

In spite of all precautions, accidents happen. When they do, what is important is your ability to quickly recover from them. Therefore, the final part of physical security management is regular and continued testing of recovery policies and procedures. This helps to guarantee safety, as well as reduce the recovery time in the event of a natural or man-made calamity.

Therefore, in order to make sure that your organization is adequately protected on the physical front, you need to ensure that these three pillars of physical security are ever-present in your security set-up. A lapse in any one of these facets can leave a loophole that malicious elements would be quick to manipulate.

The Importance of Physical Security

Cybersecurity is no doubt essential to guarantee the safe operation of your digital infrastructure; but physical security is just as important, if not more. The main purpose behind implementing physical security is to ensure that the essential business data, confidential and critical information as well as company networks, hardware and software, as well as other related infrastructure are protected.

An organization faces many forms of physical security threats, most of which can be classified in one of two categories. The first are **Natural Threats**, which constitute damage caused by natural calamities (floods, earthquakes, and the like).

In this scenario, although the information and infrastructure are not in danger of being misused or maltreated, the risk lies in the fact that such events can lead to the total destruction of your IT assets. More than the loss of hardware, the loss of years and years of critical business data can deal with a severe blow to your business operations.

The second kind of physical threat that your organization may face is that of attacks by a malicious agent; these are **Human-Initiated** events that include terror attacks, acts of vandalism, and even theft of important resources.

It is clear that ensuring the physical security of your organization is a very important part of making sure that your IT assets remain safe at all times.

Therefore, physical security measures are necessary in case you want to protect your digital assets from natural as well as man-made calamities. While there are indeed measures that you can and should take in order to protect your assets against natural disasters, the steps that you can take to protect them against intentional harm from malicious parties are also very important.

Your IT infrastructure may be attacked for a number of reasons, including personal vendetta, financial motives, or even for the simple fact that you had an open vulnerability that the attackers could exploit.

Unless adequate physical security measures are maintained, other cyber-efforts to ensure the safety of your assets become essentially redundant.

Yet strangely, this very important aspect is often overlooked by most organizations. Just think in plain terms: you can put dozens of security apps on your phone, but if you can't protect it from being snatched away then there's really no point to it, is there?

If you think about it critically, physical security is even more important in the present technological scenario. Decades ago, a single computer was the size of a small house and data storage devices were clunky machinery which could not be easily stolen.

Now, in the age of thumb-drives and mobile devices, it's very easy to lose a digital device, and along with it access to critical information and data.

Therefore, along with maintaining proper digital measures of security, physical security should also play a crucial role in the technological security landscape. Otherwise, attackers will be presented with avenues of exploitation that they can be expected to manipulate promptly. So it's imperative that physical security is maintained with the utmost diligence.

How Physical Security Helps Ensure Digital Safety

In the current day and age, all businesses are dependent on digital infrastructure for the daily running of their operations. The reason for the growing proliferation of software and hardware assets is this increased reliance on digital technologies.

Any organization's digital assets are a collection of business-critical data and documents, not to mention physical resources, that are crucial to the survival of the business. This makes it essential to ensure that apart from cyber-based countermeasures, physical aspects of the security protocols are maintained as well.

The following are some of the many ways in which ensuring the physical security of your digital assets can go a long way towards guaranteeing the safety of your IT infrastructure.

Enabling Access Restriction

Physical security measures promote safety by restricting access. This helps to segregate the levels of access that organizations impart to employees with different roles. This can be done either by allowing certain classes of employees limited access to the office space or even by ensuring that only the personnel with the appropriate authorization can access certain restricted parts of your IT systems.

This helps to boost the security culture within the organization and augment any cybersecurity measures that are already in place. Enabling proper physical security ensures that employees are not able to access parts of the organizational infrastructure which are not required for them to carry out their duties.

Such segregation of access ensures that there are multiple levels of access controls that an intruder must bypass before they get their hands on a physical resource.

Helps To Easily Isolate Breaches

In spite of all the rules put in place, there may be exceptions. Through carelessness or oversight, an unauthorized person may be able to get past your physical security measures and gain unlawful entry into, say, your server room, or be able to access a restricted part of your company network. Even in the case of such a breach, physical security measures can be of immense help.

One of the defining characteristics of physical security measures is that they are multi-layered; even if one layer of the system fails, the other layers ensure that further damage can be contained. For example, in the case of an unauthorized entry, equipment such as surveillance cameras can easily allow you to pinpoint the perpetrator.

In another scenario, ifsomeone logs into your systems with a stolen ID, you can use this information to locate which part of your organization the breach occurred and at what time.

These are only two examples that help you track any unauthorized action. Perhaps the one thing worse than a breach is not knowing who was responsible for it. When you have installed and activated proper physical security measures, your organization will be able to effectively monitor everything that goes on in your business, and in multiple ways.

Case in point: surveillance cameras let you keep a watch on every corner of your premises; another important aspect is physical checkpoints, which make use of keycards or biometric access to keep track of the traffic passing through them. This ensures there are always valid logs recording ingresses and egresses that you can check-in times of need.

Acts As A Deterrence Against Unauthorized Access

Perhaps one of the biggest characteristics of implementing physical security measures is that they are overtly visible. This is a great advantage over cybersecurity measures which are essentially invisible. It is said that what remains out of sight remains out of mind; and as physical security measures are always in sight, they are always on the top of everyone's mind.

Of course, this is not to say that you should flaunt them with an excessive display, because this itself might become a source of security vulnerability. Yet, it does help to show-off a bit. Once people know that they are under constant surveillance, this acts as a real deterrence against the intent to perform malicious acts. Let's take an example.

Suppose your organization has a server room that is off-limits to ordinary employees. In this case, some people with malicious intent may be enticed to gain access to the room physically in order to carry out some illegal activity. However, the presence of security cameras and a proper lock-based entry mechanism that requires identity verification can act as effective measures to prevent any such act from taking place.

What's more, such visible security measures also allow you to instill a sense of security in your employees; this not only improves the efficiency of your team and builds trust among them but also promotes a sense of openness within your organization.

Facilitates Faster Incidence Response Times

Many a time it is seen that the point where most organizations fail is when it comes to ensuring prompt and on-time response to breaches or incidents of harm to IT assets. This is a crucial point. In any breach of digital assets, be it natural or human-initiated, time is of crucial importance. In the event a breach does take place, having the right physical security measures allows organizations to react faster and take necessary action.

With the right level of security measures in place, companies can get real-time notifications that show you where the breach of security has occurred. This is one of the multiple benefits of a physical monitoring system. Apart from letting you know about any potential or ongoing breaches, faster response times help to reduce the cost associated with the breach.

In the above points, we have enumerated some of the broad benefits of employing physical security towards safeguarding your digital assets. With greater, more granular levels of implementation, the benefits that can accrue from correctly deploying physical security measures go far beyond mere security and enable the holistic protection of your digital infrastructure.

Now that we have a good handle on what physical security entails and why your business should be focusing on it, let's take a detailed look at some of the many physical security risks that can threaten your organization.

The Most Common Physical Security Threats

If there has been one constant in the world since the beginning of time, then it's this: you can never be too safe.

In the pre-digital age, physical security threats were the predominant cause of concern for most of humanity. Burglary then meant gaining actual physical access to the valuables in question. As a result, physical security innovations were the need of the hour.

With the advent of the digital era, however, we have been exposed to a larger number of threats that mostly originate from cyberspace. From hacking attacks to data breaches, the focus of humanity in general, and of businesses in particular, has shifted from physical security implementation to digital security provisions.

It would be wrong to think, however, that the physical risks which used to plague us are gone; in fact, as we give lesser importance to physical measures of security, we are only going to leave ourselves more vulnerable on the physical front.

With this view in mind, let us take a look at the different kinds of physical security threats that your IT infrastructure may have to address. Keep in mind that most of these threats can be targeted not only towards the digital assets of your organization but also against any other property on your premises, even your human resources.

We have already classified physical threats to organizations as natural and man-made; apart from this, based on the place of origin, physical threats can be classified as follows.

Internal Threats

These are physical threats that originate from within the organization. Examples of such threats can include careless employees, disgruntled staff members,, or even mistakes that are made by members of your security team.

Internal security threats can also come from non-human sources. For example, fires due to a faulty power supply, unwanted moisture in server farms, lack of proper cooling mechanisms all fall under the concept of internal threats. Internal threats are more

difficult to contend with than external threats because it is tougher to predict from which area you are exposed to danger.

External Threats

These are threats that originate from outside the organization, such as attacks by outside parties with malicious intent. Even natural disasters can be classified under this head. Lighting strikes, fires due to external interference, and earthquakes can all be classified under external threats.

External threats are usually more acute in nature and can have devastating effects; however, with the right levels of preparation, their damage can be limited.

While the number of individual physical threats is too many to enumerate and beyond the scope of this resource, we will take time to discuss one of the common physical security threats that can plague organizations: Theft.

This is the most common physical threat that any business must address. In the age of miniturized digital devices, you need to be extra careful about your resources, as these can be easily pocketed and taken away from your premises.

Theft can be perpetrated by internal as well as external actors. Therefore, your organization should have security measures such as RFID-enabled devices and surveillance systems that can make sure that no one is carrying out any untoward activity in your business.

When it comes to theft you have to protect against both internal as well as external threats. For businesses, the chances of employee-executed theft are far greater than external theft. Therefore, businesses should take time to understand any vulnerabilities that you might face in this regard as this will help to effectively combat these threats.

How To Mitigate Physical Security Threats

After so much discussion of physical security, it would be a crime not to know how to actually protect against some of the threats that we have learned of now.

The real question here is: what are the measures that you should implement in order to ensure your physical security? Which modes will have the greatest impact on your organization? While there is no one size fits all solution here, there are certain common measures which, when adopted and adapted according to your situation, can help protect your digital infrastructure.

Some of them are discussed below.

An Increased Number Of Security Personnel

As mentioned before, one of the best deterrents against possible attacks is visible security. This is exactly what increasing your security force guarantees. This may mean hiring extra personnel or modifying your existing patrol routes. Important entrances and exits should be manned at all times in order to ensure that no unauthorized entry or exit occurs.

Also, for guarding against theft, visitors should be frisked both before and after they visit. What's more, an additional number of security personnel give extra peace of mind to your employees and will dissuade those with malicious intent from trying to act against your business.

Of course, just having a large enough number of security personnel doesn't automatically guarantee safety. You should also ensure that your security personnel clearly understand your organizational requirements and are properly trained in the latest security protocols that your business has in place.

They should also be equipped with state-of-the-art equipment that allows them to carry out their duty effectively. They'll also be able to respond appropriately to any untoward situations that may arise.

Enhanced Monitoring Systems

In addition to augmenting your security forces, you should also take care to install, maintain and improve the performance of your surveillance systems. A well maintained and updated monitoring system can go a long way towards preventing potential dangers.

Some common practices should be carried out with this end in mind. For starters, security cameras should be placed at strategic locations so as to offer maximum visibility over your premises; this will help to greatly reduce the chances of your IT assets being compromised physically.

Another technique that can be used is an automated alert system that can notify the right personnel in case of any unauthorized intrusion or suspicious movements after working hours. This can enable security personnel to quickly respond to threats. After all, detection without response is no detection at all!

Advanced monitoring systems can also help your security teams to communicate and coordinate better. Team leaders can check the location of their guards via GPS, and ensure that the patrol teams are performing their duties properly. Also, in case of a complaint they can get to the location of the incident within a few minutes, thus ensuring speedy resolution.

Limiting On-Premise Access

Accessibility is the enemy of security, or so the saying goes. In fact, this is very true. Often, easy access to your office premises is a clarion call for perpetrators who wish to physically compromise your digital assets.

Therefore, restricting access to your premises and to important portions of your infrastructure can go a long way towards guaranteeing the protection of your valuable data and digital infrastructure.

There are many ways to ensure that only the authorized personnel gain access to your premises; apart from security personnel, using identification tags and security checks during entering and leaving the office can be effective ways to prevent misuse of your digital assets.

Another way that you can limit access is by allowing only authorized personnel with the right access codes to enter sensitive areas of your IT systems, such as server farms or critical network resources.

Improving Employee Awareness

So you have the best security systems and trained guards in place, but none of it matters if your employees are not aware of their security protocols and associated duties and responsibilities. Does your staff have the training to handle a physical intrusion into your IT systems? While this is indeed an extreme situation, it is a very likely one.

Therefore, in order to guarantee that your staff is prepared, apart from cybersecurity training, make certain that they are well trained to handle events of physical intrusions and natural calamities. Ensuring that your staff knows the standard operating procedure in case of such an event can potentially contribute towards protecting your digital systems, and maybe even save lives and property in the process.

Following the above protocols can help to create a safe and secure business environment where employees can work with peace of mind, and the management can rest assured that critical digital resources remain safe from every form of physical threat.

Top Tips To Maintain Physical Security At Your Workplace

Your digital assets and business data form the backbone of your organization. The following are certain tips that you can follow to maintain physical security at your business premises.

Keep Server Rooms Under Lock And Key

Organizations are increasingly moving towards cloud-based solutions for their computing needs, but there are still many businesses that use traditional servers that are kept on the office premises. Often, these can become soft-targets for perpetrators with nefarious purposes.

To prevent such acts, ensure that server rooms remain locked at all times and are only accessed by authorized employees. Anyone who has access to the server rooms can

potentially be a source of vulnerability. Damage or compromise of the servers in any manner can have devastating consequences for your business. Therefore, strict policies should be implemented to control access to the servers.

Make Network Devices Secure

Network devices are yet another sensitive resource that you should take utmost care to protect against physical intrusions. It has been traditionally observed that network devices are prime targets for hackers who may choose to place a sniffer device in order to siphon off important business data en route. Therefore, it is essential that you keep all network devices behind locks as well.

Ensure Proper Surveillance

Despite all precautions, breaches can still happen. In the event, such an incident does take place you need to pinpoint the person or persons who carried out the deed. In such situations, surveillance data can come in handy.

Make sure that your IT assets are placed under surveillance around the clock. For CCTV cameras, ensure that the devices are located out of easy reach so as to prevent any tampering. Also of use can be the practice of keeping logs of all people who engage with a particular resource.

Guarantee Workstation Security

Unmanned workstations are points of extreme vulnerability to your business. Potentially, anyone can use an empty workstation to log into your company systems and manipulate, steal or destroy data that is vital for your business processes.

So make sure that there are no unmanned workstations in your office, and even if there are, be certain that they cannot be accessed by anyone and everyone. This can go a long way towards making sure that your business data remains safe.

Secure Printers

Whenever we think of IT security our minds inevitably go towards computers and servers; however, output devices such as printers are also susceptible to physical threats. Many printers nowadays incorporate onboard memories that can be manipulated and hacked by experts. For example, unscrupulous persons can make unauthorized reprints of cached files containing sensitive information.

Printers, therefore, should be housed in secure locations; also, printers should be bolted to the platform they rest on in order to ensure they can't be carried away, especially if they are portable ones. Further, make sure to place a camera near the printer to ensure that all activity at the printer is recorded.

This brings us to our next tip.

Secure Portable Devices

Many businesses are nowadays shifting from traditional desktop systems to laptop computers and tablets that can be easily moved from place to place. While this ensures portability and ease of use-on-the-go, it also opens the doors for potential theft.

Portable devices, therefore, should be adequately protected in the workplace; if possible, employees should be provided with cable locks to secure the devices to their workstations. Further, motion sensors and locked drawers should also be used to prevent unauthorized access to portable devices. Security personnel at strategic entry and exit points should also be trained to frisk individuals for any devices they may bring in or take out of the office.

Protect Backups

Backups are of utmost importance, and they should be treated as such. Backups should never be kept in unlocked locations; like servers and network resources they should be kept behind lock and key. In fact, it's best if backups are stored in special locations off-premises.

Also, you should never allow employees to use personal storage devices in the workplace as they can easily make copies of backup files and take them outside the office. So make sure your security personnel are vigilant about this. You can also take greater precautions and disable all USB ports to ensure that personal devices cannot be used.

Following these tips can go a long way towards helping your business manage physical security risks.

Final Words

Amazing how time flies, and we are already at the end of our discussion. As always, we sincerely hope you enjoyed reading this resource; we sure had a great time creating it.

Humans have tried to create newer and safer security measures since time immemorial, and in the digital age, the security of IT assets has taken on an entirely new dimension. With cryptographic advances and technological interventions improving by the day, cybersecurity is one of the issues that are on the top of every business person's mind.

At the same time, it must be remembered that along with creating a safe cyber ecosystem, ensuring the physical protection of devices is also essential. Within the limited scope of this ebook, we have covered only some of the measures that can be taken to protect your IT infrastructure against physical threats; ensuring data distribution and redundancy, multiple backups, and fortification of sensitive locations are only some of the many measures that can be involved to manage physical threats.

We hope that this resource will help you towards bettering the physical security measures that are in place at your business. With the physical frontier secure, you can rest assured that your IT assets are safe and sound.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com