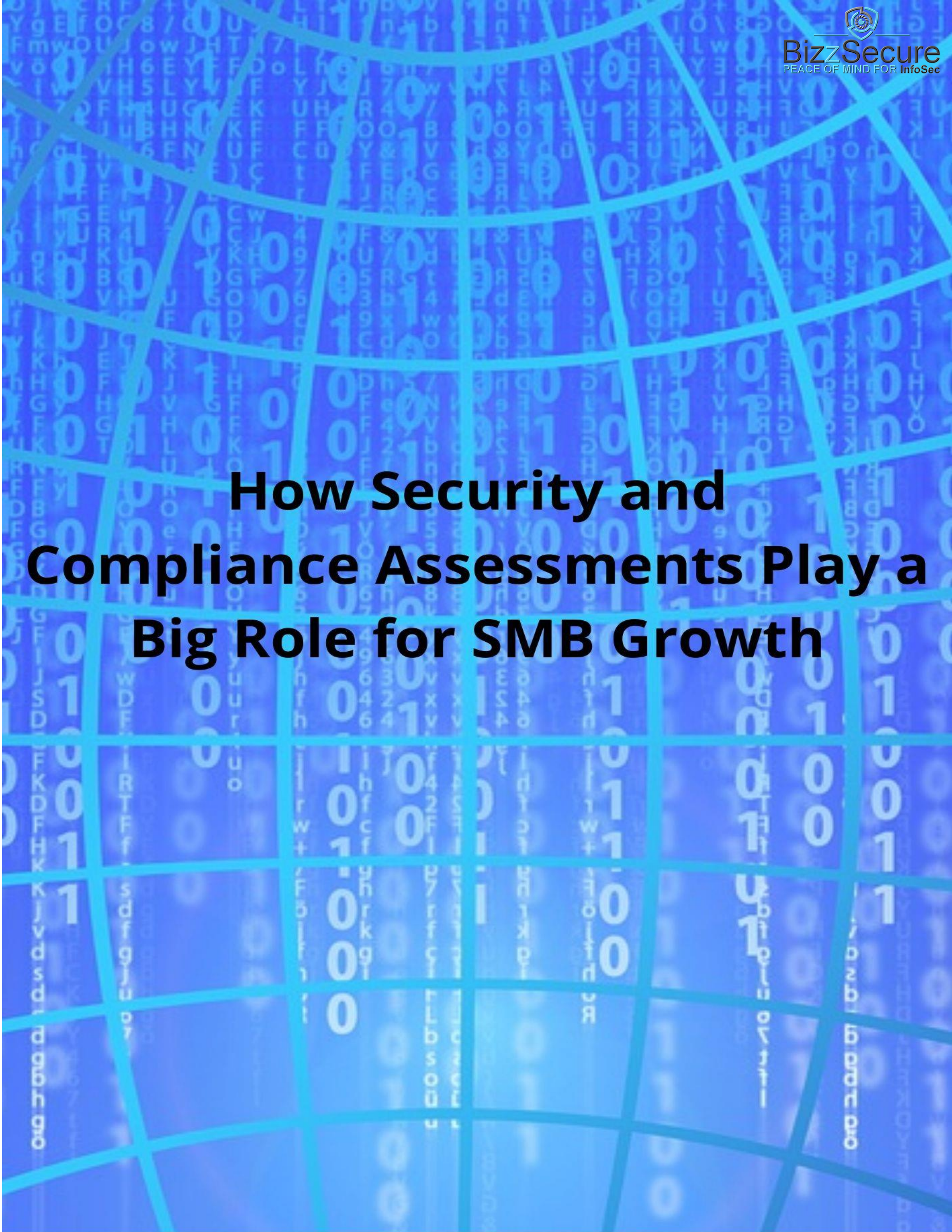
BizzSecure
PEACE OF MIND FOR InfoSec



How Security and Compliance Assessments Play a Big Role for SMB Growth

Table of Contents

Introduction

Small and medium businesses are often ignored and left in the shadow of the larger conglomerates that shine brightly on the industrial landscape. The reasons for this are understandable.

After all, large businesses employ hundreds, if not thousands of people. They have a greater economic footprint. Most of all, they have a greater presence in popular culture. This naturally makes their presence felt in a more impactful manner.

If you stop and think about it, the real story that comes to the fore is rather different. Statistics show that more than 99% of all businesses in the US are SMBs, and these employ fewer than a thousand people. By sheer numbers alone, SMBs are significant drivers of economic growth.

It would be a mistake to think that SMBs will remain in the same status for a long time. Truth is, SMBs have healthy growth rates that promise to improve their status in the economy.

This makes sense. All multinational organizations today began as small businesses, and over time they have achieved their monumental status through sheer growth.

However, as is natural, the expansion of a business is always accompanied by growth pangs, and businesses have to contend with the dynamics of growth regularly. This includes economic, staffing, and above all, security factors.

In the present world scenario, technological disruption is the biggest factor that plays a role in the making or breaking of businesses. And In the case of SMBs, this is doubly true.

Small and medium businesses don't usually have access to the large financial sources and infrastructural resources that larger businesses can utilize. As a result, they are dependent on technology to a greater extent than large businesses are. Most small businesses and startups today are technology-based.

Which makes sense; we live in the times when cyberspace is one of the biggest playing fields. Naturally, businesses are ready to fight for a piece of the proverbial pie. There is another side to the coin that businesses don't usually pay much attention to. At least, not until it's too late.

You guessed right; we're talking about security. In particular cybersecurity.

With rapid changes in the tech landscape, businesses are finding it very difficult to set up stable security standards regarding their IT infrastructure. Cyberspace is rife with threats, and businesses must remain on a sharp footing to ensure that they don't fall prey to any digital delinquents.

Naturally, this is easier for larger businesses to implement. With considerable financial and technological resources at their disposal, these businesses have the required systems in place to enable quick and easy compliance.

This very same act, however, becomes difficult for SMBs. As it is, they have to operate with limited resources. When the choice falls between running the business and complying with esoteric security rules, it's understandable which choice business owners are going to go make.

This is where most businesses make the wrong choice. When they choose the path to convenience, SMBs clear the way for greater headaches in the future.

As SMBs grow, and their operations begin to expand, they become more noticeable targets for cyber-perps. Also, since SMBs don't have as tight a security infrastructure in place, they can't protect against these attacks easily. This ultimately affects the growth of the companies.

So how can SMBs overcome this conundrum? What's the best way to ensure unhindered and sustained growth, all the while not compromising on security?

The answer is simple: Compliance Assessments. By sticking to the right compliance standards, small and medium businesses can ensure that they don't falter on the path to unhindered growth.

In today's discourse, we are going to discuss the many facets of why SMBs need to pay special attention to compliance assessment. Also to be discussed are the various security risks SMBs face, the penalties of nonconformity, and several related topics. The purpose of our discussion is singular: to understand the impact of compliance assessments on growing SMBs.

So, stick around till the end; we're sure you'll find this to be useful.

Without further delay, let's dive in.

What Security Compliance Means for Today's SMBs

It doesn't matter whether you are a large or small business. In today's times of rapid technological upheaval, the security of your IT infrastructure needs to occupy a place of paramount importance in the company policy. This is necessary not only for the safety of your business but that of your employees and customers as well.

Most businesses today rely heavily on customer data that is stored in digital systems. This can range from personal health information and financial data to identity documents and property testimonials. Ensuring the safeguarding of such data is essential for the smooth running of the businesses.

Not only is this a matter of moral responsibility, but it is also required by compliance rules set up by government agencies. These rules require businesses to follow certain standards and safeguards when it comes to ensuring the safety and integrity of their IT infrastructure.

For larger, established businesses this task is relatively easier. As these businesses already have fully fleshed out IT departments, they can quickly muster the required staff, funds and above all, practical expertise which is required to conform to these rules. Plus, they also have the resources to keep track of all changes that may take place in the compliance requirements. This, of course, is a given, considering the changing technological landscape.

However, for small and medium businesses that don't have the required compliance information, this same task can become a great hindrance to growth. At a time when they should be focusing on their business growth, if small businesses must divert time and resources to ensure conformity to myriad laws and regulations, this can pose serious hurdles in the path to expansion.

In this situation, SMBs need to first understand what security compliance means in their context. SMBs generally operate under the misconception that theirs are businesses which are immune to cyber threats. Our resources and IT infrastructure are nowhere as extensive and can therefore never be as attractive to hackers as the larger conglomerates.

While this is true (to an extent), there is another side to the coin. Just think: larger businesses have greater data and infrastructure at their disposal, which means that they are more likely to be targets of security breaches. At the same time, it cannot be denied that these businesses also have a larger amount of resources at their disposal, using which they can easily thwart off any risks that might be posed to their organizations. Any anti-legal cyber elements who plan to attack these businesses will have to think twice before they launch an attack against any of these organizations.

Small and medium businesses, on the other hand, are a different case altogether. Most often, these businesses don't have the required levels of infrastructure requirements that are needed to create a coherent action plan for compliance.

This is exactly the opening that cybercriminals look for. By sniffing out chinks in an SMB's security armor, these anti-social elements seek to penetrate them. Unlike larger businesses, which have the strength to retaliate, smaller ones can rarely survive in the wake of a cyber-attack.

Hence for businesses in the small and medium-sized category, it's essential to stick to any compliance rules that they come under. Doing so is essential not only from the security perspective, but the legal one as well.

Before going into the details of why compliance assessments are necessary, there's another, more important factor left to assess.

How do you know that your SMB is growing? Unless you are certain that your SMB is on the path to expansion, you might not be enticed enough to set in motion a compliance assessment process. Hence, it's important to understand the signs that ring out the growth of your small business.

That's what we're going to explore next.

Five Signs Your SMB Is Ready to Grow

Every business wants to grow, but it's essential in the light of security assessments to know when your business is ready for that leap of growth. The following are five tell-tale signs that let you know that your SMB is ready for the big league.

You Have More Business Than You Can Handle

This is often the first and most important indicator that your SMB is ready to grow. When you are bringing in more business than you can handle, this is a sure sign that you need to expand your operations.

While in the beginning, this might lead to certain problems such as a deluge of customers and more demand than you can supply, this poses an opportunity to streamline your operations.

Your Current Workforce Is Not Enough

The second surefire sign that your SMB needs to scale up is when you find your employees either don't have the required skills or the numbers to keep your business running.

Your Income Has Grown

When you start a business, it takes some time before it can reach a self-sustaining level. When, however, you find that your business is turning enough profit that you can run it and survive, this means that your SMB is now ready for the next level.

You Need Better Partners

A growing business means growing needs, and this naturally translates to a requirement for better supplies. When you find that your existing partners can no longer fulfill your business requirements, then you know it's time to look for better growth partners.

Your Infrastructure Needs to Be Upgraded

And this is the part which we need to deal with specifically. When your SMB can no longer be sustained on your existing IT infrastructure, then you know that your business is calling for an upgrade.

Now you need better and more computers, advanced networks and greater data processing capabilities. This means a greater reliance on digital systems.

Which, in turn, translates to a greater need for security compliance.

But why are cybercriminals so very prone to attacking growing SMBs? What are the factors that make small businesses lucrative targets for these digital delinquents? Let's take a look.

Reasons Why Growing SMBs Are Attacked

As with anything, an SMB is in a volatile state when it's expanding. There are a large number of factors at play, and business owners have a lot on their plate already. Considering all this, it's natural that businesses don't have enough time to look into compliance assessments.

This is exactly the opportunity that cybercriminals exploit. When a growing SMB falls under the dark pall of cybercrime, things spiral out of control very fast.

Another reason that SMBs are attacked lies in the ransom payment rates. As growing SMBs work on a tight budget, they require their company data to remain always available. For this reason, most SMB owners choose to pay the ransom rather than risk losing the data.

It must also be kept in mind that while SMBs do harbor a smaller amount of data than large organizations, nevertheless that data is no less sensitive. Even organizations that have less than 20 employees need to pay special attention to identity as well as financial info because these are more attractive to criminal elements.

The next point that we need to tackle is attack propagation. Small and medium businesses can't operate in isolation. SMBs have to work with other businesses and third-party operators to run their operations.

This allows attackers to use them as conduits to other businesses. Once an attacker gains access to one SMB's information, they can easily use this channel to make their way into other SMBs and even larger businesses that have dealings with the SMB under attack. This is yet another reason why SMBs are considered good targets: they allow hackers a gateway to other companies.

Due to the above reasons, small and medium-sized businesses are actually at a greater risk of falling prey to cyber infractions.

Advantages of Compliance Assessments for Growing SMBs

We've already established SMBs are not immune to cyber-attacks. On the contrary, they pose rather ripe targets for cyber-perps. Wwhile an SMB is growing, their vulnerability increases manifold.

As a result, to ensure that their growth process continues unhindered, SMBs need to rely on routine compliance assessments. It's only through regular and constant vigilance that these businesses can work towards a sustainable growth model.

The prime purpose of any cybersecurity effort remains the protection of your digital assets. Compliance assessments are yet another useful and much-required portion of the security pie.

Cybercrime has been increasing at unprecedented rates. Be it data breaches, website defacements or ransomware attacks, businesses need to protect themselves from all of these risks.

This is doubly true for SMBs that are growing, andneed careful navigation through these troubled waters. Unless SMBs are able to correctly employ the right cybersecurity assessments and practices, their attempts at growth are bound to fall flat.

Keeping the above in mind, the following are some advantages that SMBs can glean from sticking to compliance assessments during their growth phase.

Timely Identification of Vulnerabilities

Risks to your organization can be both external as well as internal, and SMBs need to protect themselves against both kinds of risks. This is exactly where compliance assessments can come in handy.

Compliance assessments help you to understand, pinpoint, and thereby remove vulnerabilities in your cybersecurity armor. They allow your SMB to understand the hidden weaknesses in your cybersecurity policies. They also enable you to create a significantly comprehensive list of the various threats that may affect your digital systems.

This allows your SMB to focus on the right measures for ensuring the safety of your digital assets. Once you have done so successfully, you can then explore methods to ramp up your security measures.

Create Proper Documentation

For any growing SMB, merely setting up a few cybersecurity policies is not enough. There needs to be a systematic documentation of all security-related policies and requirements. This allows you to create a concrete security framework that ensures perfect protection.

Compliance assessments help growing SMBs achieve just that. When you run any business, documentation plays a very important part in the day to day operations. Timely compliance assessments, carried out with diligence, can help to create the right series of paperwork that is necessary for your business to succeed.

Creates A Better Educated Workforce

For SMBs that are growing there can be no bigger asset than a workforce that is well educated in the intricacies of cyber etiquette. When you have a workforce that is aware of the essential security requirements, this allows you to focus less on employee management and more on the business side of things.

Compliance assessments can significantly help in this regard. When your workforce is well entrenched in cybersecurity best practices, and have a clear understanding of the security policies that your business employs, then they play an active part in your cybersecurity protection plan.

Another aspect that compliance assessments take care of is motivation. When your employees see that you, as the employer, are doing all that is necessary to ensure the security of your digital infrastructure, they too feel motivated and compelled to work along similar lines. By spreading a greater awareness about cybersecurity principles throughout the organization, your SMB spreads a motivational vibe throughout the business. One that your employees can't help but rise to.

This ultimately allows your SMB to walk further on the path to growth.

Prevent Before Cure

Cybersecurity compliance is not a one-off process that ensures absolute peace of mind. It's an ongoing system of identifying vulnerabilities that should never really relent.

Thus, in effect, they form a preventive measure that can allow your SMB to identify and stop cyber infractions before they even occur. This is crucial to maintaining the integrity of your digital systems.

Why is that? Because once you've been hit by a cyberattack, it becomes very difficult for any business to recover. If you're worried about the monetary implications, then consider this. Once you're hit with a cyberattack, then your business potentially faces closure. Better to spend a bit and prevent that from happening, isn't it?

Fulfills Compliance Needs

Compliance needs include periodic assessments. By carrying them out, your business will be able to evaluate the required controls that involve compliance.

Timely assessments also allow you to understand your full range of exposure. This will enable you to map and prioritize risks, and thus allocate resources to mitigate them.

Also, by carrying out regular compliance assessments, your business can make sure that it conforms to all legal requirements. Doing so can not only help your business but allow you to avoid legal hassles in the long run.

Enables Gap Analysis

Gap analysis refers to the evaluation of any critical differences between your current cybersecurity framework and any compliance regulations that you are obligated to follow. Routine compliance assessments allow your SMB to make sure that you close any holes between your current cybersecurity framework and the required compliance rules.

Facilitates Asset Discovery

There was a time when the definition of a cyber asset was restricted to a computer or a printer. Now, however, things are not so simple. An asset is no longer simply a laptop or a tablet, but rather a complex mix of digital devices and services that represents your attack surface.

This includes web and mobile applications, the cloud, and even personal devices that your employees may bring to work. A comprehensive compliance assessment ensures that you have a list of all the assets that interact with your network.

On that note, do remember that your network is perhaps your biggest IT asset. So pay special attention to it.

So now that you know the various ways in which you stand to gain from sticking to compliance assessments for your SMB, here are some tips that can allow your business to remain compliant on the path to growth.

Compliance Tips for SMBs

We think we've been able to establish the fact that SMBs are not immune to the attention of cybercriminals. The very act of thinking that small businesses are not much of a target is the kind of misconception that these criminal elements seek to exploit.

The numbers themselves prove this. As per the statistics published by the US Congressional Small Business Committee, more than 71% of cyber-attacks happen at small businesses. This proves that small businesses are a better target for cyberattacks.

Wwhy is this so? We've already visited the answer in passing, but let's repeat it for the sake of being thorough. Small and medium businesses simply don't have the required levels of infrastructure that is essential to ensure the safety of their IT systems. This makes the compliance process much more difficult for SMBs. However, the process of ensuring that your SMB doesn't fall into that same trap is not very difficult. You simply have to make sure that you follow a few best practices. The following are some tips that can help your SMB clear the road to compliance.

Educate Employees

Just as charity begins at home, the path to compliance should start with your employees. Begin the compliance process by training your employees in the best cybersecurity practices. Put in place a solid password policy, create and lay down clear ground rules for online hygiene, and enforce a strong security culture throughout the organization.

Keep Systems Updated

In general, we often tend to ignore software updates as mere nuisances. Small businesses may even view excessive updates as extra and unnecessary data costs.

Nothing could be farther from the truth. Software updates are essential security patches that are vital in maintaining the integrity of your software systems. Updates are released to plug holes in the security armor of your IT infrastructure. Hence, they are one of the most important steps you can take towards ensuring regulatory compliance.

So, make sure that you keep all your company systems up to date. By ensuring that your company computers have the latest operating system and applications, you stand to establish a solid security wall around your business that cyber threats would be hard-pressed to scale over.

Trust in Antivirus Software

Yes, we know that antivirus software is often not enough to protect against cyber-attacks. Just think: not having thissoftware won't help either.

You should keep every system in your organization protected with the latest antivirus software. Don't rely on the free antivirus packages that are available on the internet. Instead, take time to weigh multiple options and select a security suite that best suits your requirements.

Firewalls Are A Must

For small and medium businesses network security compliance can become a major headache. If your networks are exposed to the internet, then it won't be long before the criminal elements come sniffing at your gates.

To ensure that this doesn't happen, use firewalls to protect your internal network infrastructure. A firewall is essentially a combination of a hardware and software system that filters traffic to and from your internal network. Firewalls can help to bring that much-needed peace of mind to your SMB. Remember that a firewall alone is not enough to ensure compliance, at least when it comes to networks. There's another side of the coin as well, and that's what we're going to explore next.

Network Segmentation

Network architectures can and do usually follow one of two segmentation techniques. There's the flat network, that offers ease of setting up and requires less time and cost investment. However, such network architectures are very simple and therefore easy enough to breach. Once a perp gains access to even one terminal in the network, they can easily reach every system connected to the network. This means that the attack surface which the perpetrators achieve is unusually large and spread out. This makes breaches more probable.

A better solution would be a staggering network architecture, where the larger network is subdivided into several smaller networks, each of which is connected to the other but not directly. Instead, these have permissions-based boundaries which require authentication before anyone has access to it. This means that even if the attackers gain access to one part of the network, that segment can be easily isolated from the rest of the network. This facilitates containment and enforces compliance. Keep in mind that staggered network configurations are more difficult to set up and require an initial investment. They more than pay for themselves in terms of security benefits in the long run.

Beware of Mobile

Nowadays, everyone's using mobile devices at work. With desktops replaced by laptops, which are being replaced by tablet computers, workplaces are still trying to understand how mobile devices fit into the equation.

If seen in the right light, mobile devices can pose significant security risks. This is multiplied manifold when the devices deal in confidential information, such as credit card details. Another way in which these businesses can face threats is if personal mobile devices connect to the company network.

Therefore, it's imperative that you put in place the strictest of mobile device policies to ensure the safety of your company data. Measures such as not connecting to unsecured public networks, keeping mobiles up to date with the latest software patches and employing encryption are just some of the many steps that you can take to protect your SMB.

Backups Are Essential

In the digital world, backups are a sacred rule that you must swear by. This is all the more true for SMBs. These small businesses rarely have the required infrastructure to ensure that their systems remain foolproof. As a result, they often suffer irreversible data losses, resulting in significant setbacks.

To prevent this from happening, these businesses need to take routine backups of their critical data items. Keeping regular backups is one of the essential prerequisites of ensuring data security and safety. Backups can be taken in tertiary media, as hard copy, and can even be stored in the cloud.

One more thing: in case you are taking physical backups of your data, make sure to store them in data silos off-site. By isolating your data backups from the rest of the internet, you simply put another barrier between your data and the attackers.

Implement Physical Security

Often, a digital lock fails to do what a physical lock can achieve easily. Physical security is one of the most overlooked yet vital portions of maintaining security compliance.

What is physical security? It's exactly what it sounds like. Physical security is one of the most essential components of compliance conformance. Often digital security is not enough to ensure that your computer systems, data, and network infrastructure are safe.

In such cases, you need to augment your digital security efforts by including physical security measures into the equation. Physical security simply means putting your critical IT infrastructure behind lock and key. When you separate your critical IT infrastructure from the remaining of your digital systems and put it under guard, you are effectively creating a layer of protection.

Also, consider using authorization levels and authentication-based systems for enabling access to company resources such as databases and server rooms. This will allow you to keep tabs on who is accessing which system. By maintaining such a combination of physical and digital security measures you stand to enforce a strong compliance culture.

Make Wireless Networks Secure

Most workplaces, especially SMBs and similar organizations, often don't bother setting up wired internet connections and opt for wireless networks. While wireless networks do come with a modicum of convenience, nevertheless they pose a serious security hazard.

Wireless networks are inherently more vulnerable to cyber breaches as compared to wired networks. While it often takes a physical intervention to tap into a wired network, wireless networks can easily be penetrated remotely. Doing so does not even require significant tech expertise.

To ensure that such a fate doesn't befall your business, set up your router to hide the SSID. Also, make certain that your router is password protected; this adds another layer of security.

Stick to Payment Best Practices

SMBs fall under a category of businesses that utilize online payment systems to a large degree. While no law says you can't, some laws insist that you follow certain best practices when it comes to online transactions.

Your business should work with your bank and other payment processors and to ascertain that only the best tools are being used for payment processing. Make sure only top-quality tools are being used, along with proper fraud detection services.

It's best that you don't use the same computer system to process payments and surf the internet. This adds an extra layer of security.

Go POLP

No, we are not promoting onomatopoeic analogies. POLP here stands for the Principle of Least Privilege, which means employees should only be given access to as much information as they need to perform their duties.

Granting unnecessary access to employees can result in compromising the security of your IT infrastructure, and may even result in inviting pecuniary legal action.

Be Prepared with An Adequate Response Plan

Finally, in spiteofhoping for the best, you need to be prepared for the worst. No matter what safeguards you put in place, know that a determined hacker or group will surely find a way to infiltrate your systems once they have made you a target.

Be prepared with a response plan for if and when you are attacked. Keep to the compliance guidelines, and if possible, train employees using mock security drills to ensure they are conditioned to respond appropriately. Doing so can spell the difference between recovery and closure of business.

The above dozen tips are meant to be guidelines that can enable your SMB to successfully navigate the waters of compliance. By sticking to these tips, you not only ensure compliance but also enable yourself and your employees to contribute towards the growth of your business.

Final Words

We are, once again, at that part of our discussion where we must part ways. Albeit this is only for a while, still it's best to sign off with some words of wisdom.

SMBs form the backbone of the economic framework of any country. As is clear from the above discussion, they are no doubt at a greater risk of cyber-attacks than larger corporations with a greater number of resources at their disposal.

While this is indeed a matter of grave concern, what is important to understand is that SMBs aren't meant to remain small forever. Every corporate giant today began as a small business. This means that the small enterprise that you run today from your garage may very well be poised to become the behemoth of tomorrow.

It is during this critical phase of growth that small businesses need to stick to compliance assessments more assiduously. When SMBs adhere to regulatory compliance rules, they not only clear the path to their safety but also ensure that businesses dealing with them remain safe from cyber infractions.

On that note, it must be remembered that compliance assessments are a complex task that requires specialized experience and understanding of action areas. Most often, SMBs don't have the required in-house capacity to carry them out to fruition.

In such cases, it's best to employ external experts to take care of the task. Professionals with proven experience of working with compliance assessments can perform this operation with the required finesse and expertise. This can help your SMB reach the heights it truly deserves.

BizzSecure
PEACE OF MIND FOR InfoSec

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com