BizzSecure
PEACE OF MIND FOR InfoSec

How to Manage Network Security Risk

Table of Contents

Introduction

If the 21st century can be defined in one word, then it is *connectivity*.

Whether we talk about personal communication or business information exchange, the world is communicating better and faster than ever before in the history of mankind. Within the span of a few decades, human communication has evolved from working at a snail's pace to exchanging ideas at the speed of thought.

This has naturally enabled multiple facets of humanity to develop at an unprecedented rate. Whether it is remaining connected to your near and dear ones, sending important business data from one location of the world to another, to letting that friend know you are rooting for her, everything we do today is connected to others in some way.

Naturally, such extreme connectivity has been a boon for businesses worldwide. By utilizing the power of connectivity, businesses the world over have started to create an ecosystem where monopolistic voids no can no longer function.

Instead, business today has been redefined to be co-dependent; this has led to a business environment where companies, instead of competing with each other, work with each other to allow greater synergistic partnerships.

On a personal level too, communication has improved to the point where we can literally chat with someone sitting in the opposite corner of the world. Thought exchange, verbalizing ideas, and mass communication has reached levels that could previously only be found in the realms of science fiction.

What has been the cause for this unlimited source of connectedness?

The answer, again, can be summed up in a single word: *networks*.

Specifically, computer networks, which we know today like the internet, have contributed to the hyper-connectivity that we all experience. This has enabled us to be a more communicative species than ever before.

Computer networks today form the backbone of modern business. Without the internet, businesses today cannot imagine a single moment of successful operation. In fact, the way the economy is structured, you might think that before the internet, there was really no business environment.

All this is because of the network structure spread across the globe, the vast webs of data cables crisscrossing the ocean floors, and the complex mesh of computers involved in data exchange. All this is responsible for working tirelessly behind the scenes to provide us the ease-of-use and utility that we need.

Networks not only exist at a global level but also at personal levels. From companywide Local Area Networks (LANs) to pairing Bluetooth headphones, every connection is a network. In fact, the remote that you use to change TV channels also forms a network with your television. In short, networks are so ubiquitous that we barely notice them.

This is where the danger lurks.

Networks are intentionally designed to work behind-the-scenes, giving us as seamless a service as can be. Because networks are mostly hidden from our sight, they also remain absent from our thoughts when we discuss cybersecurity. When considering cybersecurity measures, we mostly depend on end-point security, i.e. ensuring the safety of the computing nodes at the end of each network connection.

This is a grave mistake.

Networks are perhaps the most vulnerable part of your IT infrastructure. Unless they are adequately protected against all infiltrative activities, there is actually no point in ensuring end-point security. It is this rather vulnerable section of your IT infrastructure that malicious online actors' intent on disrupting your business activity are most liable to target.

Yet, it is in ensuring the safety of this rather vulnerable part of the digital infrastructure that organizations often falter. The reasons behind this are many, but the prime cause is the fact that implementing network security is a complex task that requires special expertise and adeptness in handling network security issues,which internal IT teams often lack expertise in addressing.

So, what's the solution?

To help your business overcome these problems and create an environment where your networks are absolutely safe, we've decided to compile this comprehensive resource that'll guide you towards successfully managing network security risks.

After going through this resource, you'll be able to formulate a plan that can effectively help your business achieve network security and ensure that your business activity goes on uninterrupted.

As always, we’ll begin at the beginning and build up incrementally as we go along.

So, let’s start.

What Is A Network

Put simply, a network is a collection of computing devices that can communicate with each other. Much like humans who communicate using a language that every party involved in the communication can easily understand, these networks use some common rules, known as protocols, that enable devices in different parts of the world and in different time zones to effectively share, exchange, and disseminate information.

Of course, considering a broader definition, a network can be a collection of connected nodes of any nature. In fact, even your plumbing lines and electricity supply infrastructure are types of networks. For the purposes of our discussion in this resource, we are going to restrict the meaning of networks to communication networks dependent on IT infrastructure.

Let’s come back to our original discussion. Network security is of paramount importance in today’s times. Most commercial communication is dependent on network infrastructure. This makes it particularly a soft target for hackers and others with malicious intent. If any portion of your company network is infiltrated, then you stand the risk of losing information, compromising data integrity, and putting your entire operation at risk.

Therefore, it is imperative that your organization pays special attention to protecting your network infrastructure.

What are the risks that your network may face? Unless you know what threatens your network, you cannot effectively protect it. So, let’s take a look at the different areas from which your network may face threats.

Common Network Security Threats

Constant vigilance is the price of continued safety.

This timeless adage holds as true today as in the old world, perhaps more so. The internet has opened up numerous possibilities and opportunities for the business world. At the same time, it has also let loose the Pandora's Box full of cyber woes that threaten to upend the modern enterprise ecosystem.

As most of our business activities become automatized and online, we need to be extra vigilant of our digital networks. Networks form the highways through which data travels, and these must be protected from a multitude of threats to keep the world running.

With that in mind, let's take a look at some of the various threats that may affect your network negatively. While we do so, we'll also take a look at some measures that you can apply to protect your networked systems against each kind of threat.

We'll start with the most familiar threat, the computer virus.

Computer Viruses and Worms

Everyone has heard of them, and we are all afraid of them. For regular users of the internet, computer viruses are the most common network threat. As per the latest statistics, more than one-third of the global number of computers is affected by some form of malware, the most common form of which is the computer virus.

A computer virus is essentially a piece of software that is created with the intent of traveling across networks. Viruses can range from being mild nuisances that slow down your computer to extremely dangerous programs that have the potential to wreak havoc with your network infrastructure.

What is more dangerous is the fact that once a network is infected with a virus, then any device that connects to that network stands the chance of being infected. This perpetuates the cycle of infection and can lead to a viral outbreak in the cyberworld very easily.

Viruses can steal, erase and manipulate essential data, mess with your network settings, siphon off sensitive information such as financial information and login credentials... the list is endless.

Viruses usually travel via the internet, though they can also propagate from one network to another using tertiary media such as storage devices. They are destructive programs, created with the intention of infecting your core business systems, destroying essential data and making networks malfunction. Viruses usually attach themselves to a system or host file; once attached, they lie dormant till they are invoked by an activating event.

In contrast, worms are simpler programs than viruses. However, these too can wreak havoc once they enter your system. Worms can infect documents, spreadsheets, and other data files. The defining characteristic of worms is that once they enter a network, they begin to replicate themselves to the point of overloading the system resources. This leads to a fall in the quality of service that the network can provide, and ultimately results in network failure.

Worms and viruses can both form the basis for more dangerous cyber-attacks. Hence these need to be protected against at any cost. One of the best solutions is to install proper anti-malware programs on all networked devices and computers. Also, you must remember to keep your systems up to date at all times to ensure that bug fixes and software patches are always applied.

The above measures can enable network administrators to detect harmful software early on and remove them from your networks before they can cause any lasting damage.

Scamware

Scamware refers to software, which is not malware in itself but can be responsible for introducing such programs into your networks. Using scamware, scammers can lead you to believe that viruses are already installed on your system. Once they rope you in, they offer to either update your system or enable you to install antivirus software on your computer. However, the moment you try to do so, your system is actually infected.

Drive-by Attacks

This is one of the worst possibilities. Earlier, in order for your networks and computer systems to be infected, you actually had to download the infected file. Now, however, things are not so simple. In drive-by attacks, you simply have to visit any virus-infected URL and the malware is automatically downloaded to your system the moment you open the website.

Drive-by attacks allow malware to be downloaded to your systems via browser, operating system, or even a mobile app. Virus URLs are usually disguised to look like actual websites, but in fact, they are used as a trap for unsuspecting visitors.

One of the best ways to protect against these types of attacks is to keep your browser up to date. Modern browsers can usually identify malicious websites and warn the user before visiting them.

You can also use available safety tools that allow you to check the veracity of any website before actually visiting them.

Denial-of-Service Attacks

Known as DoS attacks, this kind of network threat is not really meant to harm your data but rather render your network inoperative. In a DoS attack, the target network is flooded with more packets than the network can handle. This results in overloading the network and degrading the performance of the systems. Ultimately, DoS attacks lead to network failure.

While earlier DoS attacks could be stopped by detecting the source of the attacks, in recent years they have evolved to become more dangerous. Advanced DoS attacks make use of Botnets, which are networks of computers that have been inadvertently overtaken by hackers. These botnets are generally geographically distributed. Hackers use these distributed networks to launch Distributed Denial of Service (DDoS) attacks.

In DDoS attacks, the botnets overwhelm the target network with an overload of data traffic, so much so that at one point the entire network fails. DDoS attacks are more difficult to detect and protect against as they are not launched from a single source but instead are spread over a wide geographical setting. This makes them all the more tough to protect against.

Exploit Kits

These are self-contained automated kits that are easily available on the dark web. Using these kits, hackers can launch coordinated attacks against businesses. Such attacks are usually planned in stages; first, the target network is scanned to detect any vulnerability. Once any security holes are discovered, then the actual attack payload is launched against the target.

Exploit kits are naturally designed to operate surreptitiously, and they cannot be very easily detected by traditional means. The best ways to protect against these are to put in place strong intrusion detection systems and train employees to be extra vigilant.

Ransomware

Ransomware is the latest threat on the block, and it has already made waves with the recent spate of attacks such as *WannaCry* and *NotPetya*. Ransomware usually works on the concept of system encryption. Once the ransomware enters your networks, it spreads to all systems and begins to encrypt all computers connected to the network. The ransomware then locks your device and displays a message that compels the users to pay a certain ransom amount, usually in cryptocurrencies such as Bitcoin.

Among all the network security threats, it is ransomware that has generated the greatest amount of fear and uncertainty among users. In fact, it has been estimated that a majority of the businesses that are affected by ransomware lose access to more than half of all company data permanently. Ransomware can infect secure data systems, scramble essential business information, and even delete essential files unless the ransom amount is paid.

Protecting against ransomware is, once again, a matter of employing well rounded defensive strategies. Antivirus software, updated security patches, and trained personnel are all prerequisites to ensuring that your business does not suffer the same fate as thousands of others.

Another factor that can be very effective to protect against ransomware is keeping offline backups of your critical business data in silos. This helps to ensure that even if there is a breach, your data are not completely left at the mercy of criminals who wouldn't think twice before deleting them forever.

Cryptojacking

This network security threat is intimately linked with cryptocurrencies such as Bitcoin. As cryptocurrency mining gains popularity, hackers have found a new way to exploit your network resources. In cryptojacking, hackers install cryptocurrency mining software on your organizational infrastructure and make use of your hardware and network resources to mine cryptocurrency.

This will certainly impact the performance of your IT infrastructure. Usual signs are sudden data spikes, a slowing down of your network infrastructure, and overall sluggishness. Unless companies understand the real cause of the problem, they might end up wasting a large amount of money in making unnecessary upgrades.

In order to defend against cryptojacking, it is essential for your IT experts to continuously monitor all network activity in your systems. Any unnatural behavior should be immediately looked into and resolved to complete satisfaction. In terms of architecture, cryptojacking software is exactly similar to viruses or worms; the only difference being that their ultimate goal is to use your hardware resources. Therefore, general preventive measures that work for malware are also applicable to cryptojacking.

Advanced Persistent Threats

Naturally, we’ve kept the worst for last.

APTs are a form of network attack in which the malicious attacker program gains access to the network and hides there for an inordinate amount of time. However, the most important difference between APTs and other malware is that while regular viruses and malicious software manifest themselves in some form of system anomaly, APTs are designed to be undetectable. Rather than damage the system they have infected, APTs instead remain silently active. They quietly collect all data and sensitive business information that flows across your network and siphon them off to the perpetrators.

APTs can enter your networks through a variety of means, such as malware and exploits. Once an APT gains access to your company systems they can efficiently scan and infect critical parts of your infrastructure. This ultimately leads to a leakage of data across your entire network.

Protecting against APTs requires, once again, the same efforts to be made as for other network threats. While it is true that no system can be entirely safe, yet by keeping to best network security practices you can ensure that your business networks are protected from harm due to these malicious agents of destruction.

This is where network security risk management enters.

The Importance of Network Security Risk Management

Most C-suite executives lose sleep over network security but are still unsure of what to do. Network security measures typically require substantial upfront costs and the threats that an organization faces seem to be so multifaceted that they can’t be anticipated.

However, it must be remembered that waiting to act until after the breach can be akin to asking for medicine after the patient has died. In general, it has been estimated that every organization faces at least two random cyber-attacks on any given week, and once a breach actually occurs it can take months, and potentially even years, to fully recover from the effects. Not to mention the number of resources and money that must be invested to repair the damage.

Therefore, the wise course of action is to take a proactive measure and fortify your network defenses against all probable and possible attacks. The good news here is that most coordinated cyber-attacks follow a predictable pattern. Cybercriminals often use the same modus operandi to steal data or gain access to financial information. With a systematic approach to network security management, these attempts can be easily thwarted.

Therefore, instead of looking at stopgap measures to protect your network assets, you need to ensure that your business takes an in-depth approach to network risk management. Ideally, an organization can choose any of the following courses of action when it comes to risk management:

- Choose to avoid risk by eliminating the possibility of an attack.
- Minimize exposure to potential attacks.
- Distribute the risk between departments and organizations.

When it comes to network security, the risks are multifaceted. Therefore, risk management efforts must look at the broader picture, and work towards reducing the risks that plague an organization. The key to successful network risk management for organizations lies in the careful estimation of risks and their ranking according to potential damage. Once the risks have been identified, methods to overcome them must be formulated.

As with the risks, the methods to overcome them are also multifaceted. Some of these require technical expertise and demand domain knowledge and experience, while others can be effectively applied with the right form of training. Employee training is one of the proven methods to secure network security, especially at the endpoints.

For best results, however, companies should consider hiring network security experts who have proven and demonstrated experience in handling network issues. Often, a private firm can provide independent professionals whose unbiased eyes can be helpful in mitigating risks.

Risk Management Solutions

Network security risks are not necessarily an insurmountable barrier. Putting proper network security risk management plans in place doesn’t need to be an exercise steeped in complexity. Preventing network breaches is simply a matter of maintaining constant vigilance. The following are some methods that can be utilized to implement a sound network security policy in your organization.

Enable Access Control

Effective access control is one of the most important parts of network security. Lack of access control may be akin to leaving the doors open and inviting in the criminals. Access control can be implemented in a number of ways, both physical and digital.

In terms of digital security, appropriate password policies, role-based access enablement, and implementing POPL can be effective measures. POPL (Principle of Least Privilege) is the practice of granting employees only that much access as is required for them to do their job effectively. By doing so, you minimize the chances of unauthorized access and therefore restrict the damage that may result from the same.

In terms of physical security, a regime of well-trained security personnel, barriers to essential network resources, and the creation of sound security culture are some of the steps that you can take. For a detailed guide on how to implement the right physical security measures, check out this resource here.

Remember to Be Updated

Aren’t updates annoying?

Most of us seem to think so. Actually, these pesky alerts can be vital to the health of your network infrastructure. From the anti-malware programs that you use to the operating systems running your networks, guaranteeing that your software is up to date is one of the most essential steps that you can take to ensure your network safety.

Usually, when a new version of the software is released, old bugs and security holes are patched. This means that old security vulnerabilities can no longer plague your network infrastructure. Most people fail to update their systems, and this lets the hackers have a field day. In fact, it is estimated that the lack of proper updates is the cause of more than half the network breaches that occur in any business.

Therefore, take care to always keep your network resources updated. Enable automatic updates where possible and be sure to download and install the latest patches whenever they are released.

Introduce Standardization

In larger organizations, there are bound to be a number of systems running a variety of software programs. However, it must be looked after that the software which is being used in your network is not derived from dubious sources. In fact, it's best that account control measures are introduced at every endpoint and software installations are strictly controlled. Also, employees must be encouraged to seek prior approval before installing any applications.

Not knowing what software runs on your networks is tantamount to network security sacrilege. This can introduce huge security holes in your security infrastructure. Ensure that all your systems are using uniform application software, and any deviations are strictly monitored and controlled.

Ensure Network Protection

Protecting your network is paramount to the success of your business. In order to do this successfully, you must keep in place proper access controls. Enabling firewalls, using virtual private networks, and regular network maintenance are some of the many measures that you can take to protect your network infrastructure.

Trained Personnel Are A Must

Often, external threats are successful because of internal weaknesses. A workforce that does not follow proper network security practices can be your greatest liability. In fact, the weakest link in your network infrastructure has to be the human element.

In order to protect your network assets, make sure that your employees understand network security. Also, employees should be adequately trained to be able to identify threats before they snowball into major breaches. Further, make sure the employees are aware of the right contact person to go to in case of a breach.

Therefore, be certain to provide network security training throughout the year and ensure that you keep your employees abreast of the latest security practices. As time flies, network vulnerabilities change. Your workforce should be able to keep up with the same and be ever vigilant.

In case you feel that your existing workforce is not adequate to handle the risks your business faces, contact external professionals immediately. When it comes to network security, time is of the essence. Professional network security experts can provide valuable insights and take timely action to protect your resources. Therefore, do not delay seeking help when you really need it.

Implementing the above measures can guarantee that your network resources remain safe and secure at all times. True, putting all the above measures in place may require an intense amount of effort, vast resource investment and above all, the stolid dedication that can only come from experience. In the end, all this is necessary to protect your network resources.

Keep in mind, however, that lackadaisical implementation of these steps is not sufficient to ensure network safety. In fact, this can do more harm than good.While implementing the above steps, take care to go all the way and enforce them with integrity.

Advantages of Network Security Risk Management

Now that we’ve discussed network security threats at length and also gone through certain methods to ensure proper network management, now it’s time to look at some advantages of a good network security risk management plan. Knowing the advantages that you stand to gain from the correct level of network security can help to give your business the right impetus to incorporate the same.

Of course, it goes without saying that the first and foremost benefit of network security risk management is to introduce a minimization in the level of threats that your organizational network faces. For many businesses, however, achieving an adequate level of security can be a tough call without external professional help.

The right network security measures, when put in place, also help to keep business-critical data and financial information safe from prying eyes. This allows you to reduce the impact in case of a data breach, and also ensures that your business is not penalized for lack of regulatory compliance. Fines for non-compliance can be hefty, and your business can suffer a serious setback when exposed to such punitive measures.

Apart from the above, the following are some other benefits of network security risk management.

Improved Client Confidence

A sound network security management program helps your clients know that you are doing your due diligence in protecting their information. This naturally leads to an increase in the client confidence level. As clients begin to view you as the gatekeeper of their digital resources, their reliance on your business naturally grows. This has the effect of their becoming vocal patrons who remain loyal to your services and offerings. Not only does this lead to increased business but also it helps to improve your market reputation.

Better Regulatory Compliance

As discussed above, the lack of proper network security management leads to decreased compliance, which can result in several legal and financial penalties. Keeping the right network security measures in place can enable your business to adhere to the highest regulatory standards and avoid steep penalties. By introducing real-time monitoring of data flows across the organization, your business stands to enhance its compliance posture.

Productivity Boost

One of the hallmarks of a lax network security policy is employees spending too much office time on online recreational sites. Social media, online shopping, and chat platforms are all proven productivity killers. By putting a strong network security policy in place, you can ensure that your business promotes safe and secure online habits by stopping access to these websites.

Further, certain recreational sites such as adult entertainment and piracy hotspots are known breeding grounds for malware and related anomalies that can make their way into your company systems without the visitors having any inkling of this happening. Therefore, by introducing the right network security measures you can ensure that your business is free from these troubles. This ensures that your employees are not distracted by such dubious means of entertainment, thus allowing them to focus on the job at hand.

Improved Profits

This one, obviously, goes without saying. A solid network security policy means a lesser risk of breaches, improved client confidence, and better business practices. All of these coupled together create the right environment that enables your business to improve profits. Also, a sound network security policy helps your organization avoid penalties for non-compliance. This also results in significant cost savings. In short, it goes without saying that improved network security risk management leads to better profits for your business.

Finally, all of the above points culminate in one significant advantage: that of introducing a culture of safety. By inculcating the right security habits in your employees across all levels of the organization, you can ensure that your business does not lack any of the essential security measures and continues to function at par with the latest safety standards. This ultimately affords you peace of mind and a sense of safety.

Final Words

Once again we find ourselves at the juncture where we must bid adieu. As always, we sincerely hope that you have enjoyed and benefited from the information imparted in these pages. It is, after all, our ultimate goal.

We want to leave you with some more food for thought.

Humans, as a species, cannot thrive without networks and communication. In fact, these are two of the hallmarks of human civilization. Long before computers and the internet, humans were networking with each other in myriad ways. Be it building roads or creating means of information exchange, networks have always formed a major part of our information interchange mechanism.

Consequently, the protection of these networks in multiple forms has also been one of the defining characteristics of human culture. Encryption, cipher technology, and network protocols have all sprung from the need to make networks safer and more impenetrable.

In the 21st century, however, network security has taken on a whole new meaning. The digital world has opened the vistas to a large number of business opportunities. Along with that has also paved the way for a new breed of threats that seek to upend the current business landscape.

Cyber threats and breaches are no doubt the scourge of modern times. As businesses seek greater dependence on digital networks for their operation, these malicious forces are relentlessly developing more sophisticated methods to penetrate into business networks and render them inoperative.

Therefore, to protect our present networks and consequently our way of life, we need to create an environment of safety that ensures the secure and seamless functioning of our network resources. By doing so, we can guarantee that the world is safe, and humans can continue to network with ease.

To end with what we began: connectivity is the watchword of the present times, and we as a species stand to gain more from connectedness than isolation. Therefore, we need to protect our network resources at all costs.

That’s all for now. Until next time, stay connected.

BizzSecure
PEACE OF MIND FOR InfoSec

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com