

EBOOK

A Guide to Cybersecurity

**Why a Managed Security Provider is the
Best Bet for Your Business**

Table of Contents

- 03** Introduction
- 06** Who is at Risk of Cyberattacks?
- 08** The Most Common Types of Cyberattacks
- 14** The Solution: Creating a Network Security Plan
- 21** Why Your Business Needs a Cybersecurity Plan
- 26** Working with a Managed Security Service Provider
- 30** The Takeaway



Introduction

Cybercrime is on the rise, and so it's now more important than ever to take proactive measures to protect your business against imminent cyberthreats. According to findings published in the [End of Year Data Breach Report by Identity Theft Resource Center](#), the business sector is the main target for data breaches and hacking attempts. The report also shows that in 2018 alone, there were well over 1,000 cases of data breaches in which more than 400 million sensitive records were exposed, with criminals hitting everyone from banks and healthcare facilities, through to learning institutions.

But cybercrime is not only a security threat. It is also a growing business in itself. It is estimated that cybercriminals make at least [\\$1.5 trillion every year](#) from extortion, ransom, and the illicit trade of stolen business, financial, and personal information. The global cybersecurity industry, on the other hand, is currently valued at [just over \\$160 billion](#). This discrepancy demonstrates how attractive the current status quo is for cybercriminals.

Cybersecurity has become such a serious concern that the World Economic forum listed cybercrime as one of the top five risks to global stability in the [2019 Global Risk Report](#).



These statistics are not meant to instill fear in the hearts of entrepreneurs and business leaders. Instead, they should give organizations a clear perspective of just how severe cyberthreats have become, and help them to take appropriate action.

Besides, in most cases, people never really ponder over such statistics until they become part of the figures themselves. In other words, cybercrime becomes apparent to most businesses only once they fall victim to attacks – and, by then, it's too late to take meaningful action.

Sadly, this is the gravity of the problem that modern businesses have to deal with, and many don't even realize it. These are the very issues we hope to address in this article. We analyze cybersecurity challenges in-depth – describing the various methods cybercriminals use to launch their attacks, who is at risk, and the effective solutions in place to prevent and mitigate cyberthreats.





CHAPTER ONE:

Who is at Risk of Cyberattacks?



To be brutally honest, any business that handles, stores, or uses sensitive data, whether locally, or remotely on cloud systems, is at risk of cyberattack. The threat is greater for businesses using remotely accessible network services, including the internet and local network facilities.

Both big and small businesses have roughly equal chances of being attacked. According to [a report by Verizon](#), 43 percent of cyberattacks in 2018 were targeted at small and medium-sized enterprises. The report also goes on to show that a majority of attacks (69 percent to be precise) are perpetrated by outsiders, meaning that internal attacks are not only possible, but in fact quite common.

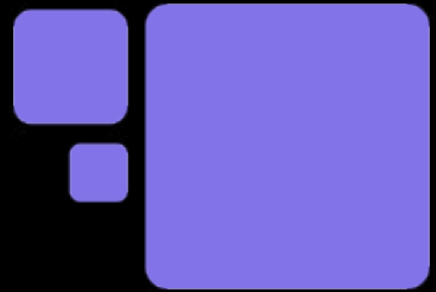
Attackers may have many different motives for victimizing a particular company. Most are after monetary gains; others are only out to sabotage business operations and IT resources, maybe to prove their hacking skills or drum up business for competitors. It's not unheard of for business rivals to take their duels to the digital space.

Don't take comfort by assuming that you have nothing to lose in an attack, or that you're a small target – you never know who has it out for you. It is imperative to keep your guard up to avoid succumbing to attacks; don't take any chances with cybersecurity.



CHAPTER TWO:

The Most Common Types of Cyberattacks



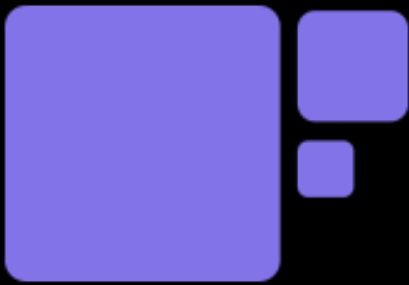
Cyberattacks can range from simple nuances to devastating data breaches that bring a catastrophic halt to business operations. The recent wave of cyberattacks and emerging threats have got security experts reconsidering their perceptions of the typical cybercrimes and their perpetrators.

Threats are becoming more sophisticated, more carefully engineered, and better organized. It seems that cybercriminals are investing their resources and time into perpetrating their heinous acts. Here is a description of some of the most common cyberattacks to give you a glimpse into the kind of threats you should prepare for.

Malware Attack

Malware is an inclusive term that describes malicious software such as viruses, worms, trojan horses, spyware, and ransomware. Malware is typically installed by unsuspecting users who click on infected email attachments and files. Once the malware is introduced into the host system, it can then go on to do whatever it was designed for; it could be corrupting information in databases, collecting passwords, or creating new vulnerabilities to facilitate an even more aggressive attack.

Robust firewalls and anti-malware tools can stop most malware before they're even installed. Malware bears a digital signature that's easy to identify and distinguish from other applications (at least in computing terms). You may also have to encourage cyber-hygiene among your employees to stop them from opening suspicious email attachments and files.



Dos (Denial-Of-Service) Attack

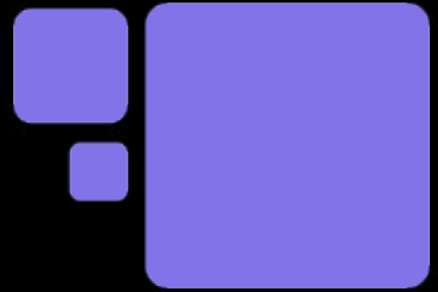
In a DoS attack, the attacker sends multiple requests to a network or server system in an attempt to flood the network traffic and overwhelm servers. Once the system is successfully overloaded, it is rendered unresponsive and unable to serve its purpose of fulfilling legitimate requests.

In most cases, the attacker asks for a ransom to be paid in order to stop the attack. DoS attacks may be old-fashioned, but they are notoriously difficult to anticipate, prevent, and mitigate. However, intelligent network traffic management systems and network security measures help prevent and identify such attacks.

Man-In-The-Middle Attack

A MitM attack, also known as an eavesdropping attack, is a somewhat stealthy tactic where the attacker sits between two or more communicating parties without their knowledge and listens in on their exchange. Such attackers have been known to intercept phone calls, emails, and other communications by exploiting security vulnerabilities in the network or deploying spyware. The goal here is to collect trade secrets, business information, and even security credentials.

To prevent this type of attack, every communication channel has to have end-to-end encryption or encapsulation protocols to keep hackers from deciphering intercepted information should they manage to get hold of it.



Phishing

Phishing is a common social engineering attack aimed at unsuspecting users to persuade them to willingly share sensitive information such as banking details, passwords, and authentication credentials. They are typically carried out through emails, and they are actually quite successful most of the time.

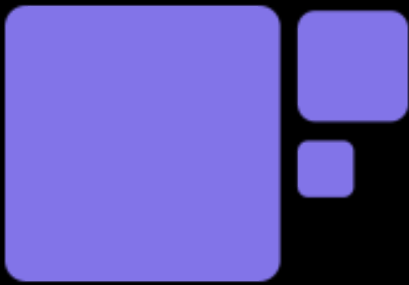
Phishing attacks mostly prey on the naivety of internet users, so there is little you can do in the way of preventing phishing, apart from training your employees on how to identify phishing activities.



SQL Injections

SQL injections are some of the simplest tricks in the cybercriminal's handbook. The attacker feeds malicious code to the back-end database of a website or online app by simply typing and submitting arbitrary SQL code on forms and input fields. The code can then manipulate the database in favor of the attacker.

Such attacks can only be stopped by securing the back end, as well as imposing strict input protocols on the end-user application. For instance, requiring input data validation on the fly before it reaches the database, and managing “dangerous input characters.”



Inside Job

An insider attack is any threat that comes from within the organization itself. Such an attack can take just about any form, from data theft to sabotage. Most inside jobs are only identified once they've already happened or while in progress.

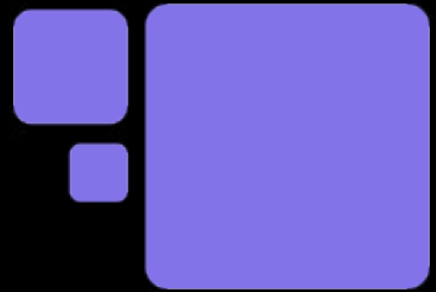
You can only discourage staff members from perpetrating inside attacks by strictly regulating authorizations to data access points, and IT controls. You should also implement an accountability system in the workplace that holds employees and shareholders responsible for actions jeopardizing data security.

Password Breaking

Password breaking is probably the oldest form of cyberattack. Although authentication systems are much smarter today and able to detect and resist most password hacks, the systems are only as secure as the passwords used. Follow security-focused password guidelines when creating and using passwords, especially on sensitive accounts and profiles. It also helps to have multi-factor authentication (MFA) for absolute user validation.

AI-Powered Attack

Cybercriminals are now using artificial intelligence to design dangerously sophisticated malware. AI-powered malware can remain undetected in a host system for months, and can even corrupt security systems. AI attacks are a scary prospect, although they are quite rare and a bit unrefined at this point, but not any less threatening. The answer to AI attacks is AI security, and although AI protection is relatively expensive, it goes beyond mitigating intelligent threats.



IoT (Internet of Things) Attack

The concept of IoT is relatively new, but IoT devices and networks have quickly become hot targets for hackers. IoT devices link together and communicate through the internet. This technology is key to modern business automation. However, IoT security protocols are unstandardized, which creates critical security vulnerabilities. A new report shockingly reveals that it is possible to hack many IoT-enabled devices in under five minutes!

The method of securing IoT systems depends on the devices themselves. At least for now, don't rely so much on these devices' embedded security features.

Cryptojacking

Cryptojacking is another emerging threat that is quickly making its way to the headlines. Crypto mining is a resource-intensive process, and hackers have found a way to piggyback on corporate computing systems to do the mining for them. A single cryptojacking attack can slow down the entire IT system. The attack bears similarities to a DoS attack, and it is actually often mistaken for the latter. But unlike DoS, cryptojacking drains processing power and memory instead of jamming the network bandwidth.

To protect your IT systems from cryptojacking, you have to seal off vulnerabilities that can lead to the exploitation of your hardware resources, such as servers and workstations. Also, keep an eye on your IT performance and track spikes and fluctuations in processing outputs and power usage.





CHAPTER THREE:

The Solution: Creating a Network Security Plan



Although cybercrime is clearly a serious business security threat, a majority of businesses are still inadequately prepared to deal with cyberattacks. A [recent survey](#) that involved 3,000 business leaders from various parts of the world revealed that only 39 percent of business executives had confidence in their company's cybersecurity. 59 percent of the respondents felt that they were insufficiently equipped to handle modern threats.

The solution to cybercrime is creating a robust network and cybersecurity plan. However, building and maintaining a digital security strategy is not easy for most businesses. We've outlined some of the key considerations for implementing dependable cybersecurity in your business.

Asses Vulnerabilities

The first thing you need to do in creating a cybersecurity plan is to conduct a vulnerability assessment. This is a thorough process of identifying and analyzing potential security loopholes in the entire IT infrastructure, whether locally or remotely. You'll have to examine and test your network, IT hardware, data access points, online platforms, software, and even your staff for vulnerabilities.

A vulnerability assessment provides you and the shareholders with actionable information on the current state of cybersecurity in the business, areas that need improvements, and the necessary changes that must be made. This information should help you formulate a budget, timeline, and goals for your cybersecurity plan.



Consider a Managed IT Provider

A managed IT provider is a third-party contractor who manages and controls IT resources on behalf of a business. Managed IT providers are tasked with ensuring the availability of business IT services and resources through IT support and maintenance.

Most managed IT services also offer remote and in-house network security and data protection; some even specialize as managed IT security service providers (MSSP).

MSSPs provide businesses with various services regarding cybersecurity, such as IT monitoring, implementation of firewalls and anti-malware, intrusion detection and mitigation, data encryption and backup, and secure communication. The range of services depends on the MSSP and the security demands that must be met.

Managed security is the one-stop security solution for both large and small organizations. The advantage is that you get professional services and robust security solutions at an unbelievably low price compared to other alternatives.

Get Everyone on Board

Many organizations often ignore the human factor when implementing a cybersecurity plan. Even the most effective cybersecurity system will serve little to no purpose if your employees and business partners don't agree with its principles.



Run the proposed changes and security measures by the people it concerns and make sure that the plan is well understood, and everyone learns and agrees to their roles and responsibilities. Implementing a security plan often means changes in administration, access protocols, and end-user devices; you should expect some friction if certain groups or individuals feel disadvantaged by such modifications. It's your responsibility to assure everyone that the anticipated or ongoing changes are for the greater good of the company.

Educate Your Employees

Your employees are the first line of defense against cyberattacks; however, they may be the weakest link in your organizational security plan. Staff members who handle critical data and IT systems can either make or break your security plan. In 2018, about [30 percent of small business owners](#) who suffered data breaches attributed the causes to human error.

The only way to avoid innocent mistakes from causing untold losses is to cultivate a dynamic security culture in the workplace. Train your employees in cybersecurity essentials like general cyber-hygiene, strong password policies, what programs to download, websites to avoid, and being accountable for data security. Inform your employees how careless mistakes like clicking on unverified email attachments can put the entire company at risk. The goal is to turn your staff into security advocates for the business.



Create Strict Access Protocols

Besides educating your employees on cybersecurity, it would also help to further reduce employee-related risks by narrowing the scope of data and IT access in the workplace, and outside the business premises as well. Entrust only a few responsible individuals with high-level clearance to access, manipulate, and use secured data and IT resources. And even then, limit just how much control each person has, in order to instill accountability.

Strict access control is particularly vital in remote systems because you never know who might be on the other end. However, thorough user identification, verification, and authentication methods can help reduce the risk of identity theft and system intrusions related to remote access.





Invest in the Latest IT Solutions

Your MSSP will probably advise you on any necessary upgrades to your IT systems, including hardware, client applications, anti-malware, and system software. Keeping up to date with new IT and security tech is essential in combating cybercrime.

Older systems are generally more vulnerable than the latest installments. For instance, newer versions of software applications usually come with updated security patches and more secure user features than their previous releases, which means they are more capable of dealing with newer threats. The same goes for hardware components, communication systems, and network facilities.

Think About Data Backups

Data availability is a big part of data security. The only way to guarantee data availability on-demand is to implement a dependable backup and disaster recovery system. Most businesses opt for cloud-based backup solutions since they are cheaper, more convenient, and in most cases, more secure than on-prem storage facilities. However, there is no problem with housing your backup locally as long as you have reassuring measures in place to handle local storage and backup challenges.

The 3-2-1 backup rule is an effective and easy-to-implement data backup strategy. Following this rule, you should have at least three copies of your data, store two copies on different media, and store one copy offsite. The crucial considerations for your data backup strategy should be frequency, security, and recoverability. Backup your data regularly (preferably as soon as it is generated) in a secure facility with quick recovery options that do not interfere with the data's integrity.



Besides cyberattacks, small data entry mistakes and natural disasters can cause temporary or permanent data loss and unavailability. A backup is invaluable in such situations.

Monitor Your Security Performance

Implementing a cybersecurity plan is not a one-off activity. The cybersecurity landscape keeps changing as cybercriminals find more ingenious ways to steal data. Cybersecurity techniques also evolve incrementally to keep up with crime trends. Therefore, you'll need to keep adjusting your security approach in order to reinforce your strategy.

Monitor your IT systems constantly and examine your security performance regularly to make sure that every shield holds. A managed IT provider can guarantee 24/7 monitoring of your systems to ensure that everything stays in the green.

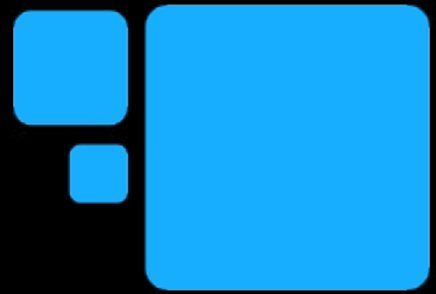
Monitoring helps identify incoming threats, and pinpoint emerging vulnerabilities and security loopholes before they become a problem. Plus, constant vigilance keeps the overall health of the IT infrastructure in check.





CHAPTER FOUR:

Why Your Business Needs a Cybersecurity Plan



Without an effective cybersecurity plan, you expose your business to the risk of cyberattacks. We've already seen that attacks can take a variety of forms, and attackers can target just about any business. Cybercriminals are mostly after business information, which they then sell in the black market or hold for ransom – this is how most data breaches play out.

Every organization is unique in terms of how it can be affected by a data breach. However, there are some common impacts of cyberattacks and data breaches that affect organizations across the board. Here are three convincing reasons to fortify your cybersecurity strategy.

Avoid Costly Payouts and Consequences

According to [recently released statistics](#), the cost of data breaches is growing. There is still a lot of speculation and debate about the actual cost of data breaches. One report puts the average cost of a single data breach at roughly \$3 million, while some analysts say it can go as high as \$8 million.

Putting the figures aside, what really constitutes the cost of a data breach? First, there is the cost of ransom, which depends on the amount of data and how valuable the hacker thinks the data is. Data ransom can range from a few thousand dollars to millions. This money is unrecoverable and untraceable since cybercriminals insist on receiving in cryptocurrency, particularly bitcoin.

Second, there is the cost of halted business processes and downtime on account of the attack. Severe attacks can paralyze critical business operations for days and even weeks, leading to huge losses, both in terms of cash and in terms of lost business and reputation.



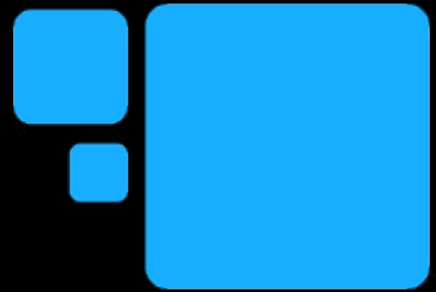
Finally, you should expect lawsuits after a data breach or data leak depending on the nature of the data involved. As a business, the law holds you responsible for protecting sensitive user data. Users whose data falls into the wrong hands have a right to sue for damages such as exposure and identity theft. Such cases can drag along for several months and consume thousands of dollars in legal fees and representation along the way, not to mention the cost of settlements and the possibility of class action.

You can never accurately predict how much a data breach could cost your business until it happens. And if it does happen, it will probably be seriously expensive.

Comply With Legal Guidelines

Depending on the nature of your enterprise and the kind of data the business handles, certain data protection and privacy legislation may apply to you. American companies are expected to comply with state, federal, and international data security laws, examples include:

- California Consumer Privacy Act (CCPA) 2018
- Cybersecurity Information Sharing Act (CISA) of 2015
- Federal Exchange Data Breach Notification Act of 2015
- General Data Protection Regulation (GDPR) 2016
- Gramm-Leach-Bliley Act (GLBA) of 1999
- Health Insurance Portability and Accountability Act (HIPAA) of 1996



- Homeland Security Act/ Federal Information Security Management Act (FISMA), of 2002
- Payment Card Industry Data Security Standards (PCI DDS) 2004

Compliance with these laws demands to put in place acceptable cybersecurity measures that guarantee data protection and privacy. While formulating a cybersecurity plan, you should align the security strategies with the legal guidelines imposed in your business niche or industry.

Failing to comply can attract hefty fines and other penalties. With HIPAA, for instance, fines for exposing a single medical record can range from \$50 to \$50,000, and organizations and officers pay \$100,000 and \$10,000 in fines respectively for violating GLBA law.

In addition to requiring monetary fines, the authorities can take further action, such as suspending the business license or withholding certain permits. In some cases, business executives may even end up in jail for ignoring or refusing to abide by specific laws.

“In addition to requiring monetary fines, the authorities can take further action, such as suspending the business license or withholding certain permits.”



Maintain Brand Reputation

Even more overwhelming than the financial losses is the loss of brand reputation resulting from a cyberattack. Customers want to interact and do business with companies they can trust; a data breach shows that the brand cannot be trusted to protect customer data.


This comes as a severe blow to the brand; victimized businesses struggle to shake off the bad image and restore the broken trust. In most cases, the tarnished image of the business lingers on, and leads to drastic decisions such as rebranding and assimilating into an existing company. Some are not fortunate enough to have these options, and end up closing shop for good. Loss of customer base, trust, talent, and reputation, coupled with substantial financial losses, leaves many businesses with no choice other than to liquidate assets and dissolve the company.





CHAPTER FIVE:

Working with a Managed Security Service Provider



A [2019 report compiled by Zogby Analytics](#) found that a third of companies suffered heavy financial losses within 12 months of experiencing a data breach, while 25 percent filed for bankruptcy, and 10 percent went out of business altogether.

We've mentioned partnering with an MSSP as part of formulating a robust cybersecurity plan, but what does it really mean to have an MSSP by your side? What benefits should your business expect from outsourcing IT and data security to a managed security service provider?

Remote Monitoring

MSSPs have the tools, resources, and manpower to track and monitor IT services and activities remotely, around the clock. Modern IT resources are often decentralized systems that reside in different locations and are synchronized through networks and the internet. Keeping a close eye on these systems is crucial in assessing security performance. However, IT vigilance is a daunting task for many businesses, but a piece of cake for dedicated security services.

Remote monitoring helps identify any unusual activities or traffic in the network indicative of imminent cyberthreats. Monitoring also helps narrow down on IT performance bottlenecks and vulnerabilities and find prompt solutions to patch security weaknesses and poorly performing components through upgrades and IT servicing.



Security analysts are adamant that a majority of cyberattacks can be stopped if identified early enough. Remote monitoring gives your business a sort of early warning system. Identifying and confirming threat suspicions on time can make all the difference in your cybersecurity efforts.

Cost-Saving


An MSSP can help your business save money in several different ways. For starters, a managed service provider costs a lot less than an in-house IT department, which considerably lowers the cost of IT support, maintenance, and security.

Since the MSSP ensures that all the IT systems work as expected, there is very little chance of downtime resulting from service or data unavailability. System downtime in an IT-dependent business environment could mean massive losses in just a short time.

You also save operational costs with an MSSP, since you only pay for the services you need. This makes your IT budget incredibly efficient and gives you more value for your money. The good thing is that you can always scale your managed services up or down to meet new demands or further cut costs.

Proactive Security

Measures MSSPs are highly skilled and experienced in cybersecurity. As such, they can easily deal with whatever cybercriminals throw at your business. Some MSSPs have proprietary security tools that they use to protect their clients' systems. This goes to show just how seriously they take their work and responsibilities.



A managed security service provider will continuously monitor your information systems to find new ways of improving data security. It's that level of dedication and innovative will that's needed to combat modern cyberthreats.

Improve Productivity

Your IT performance means a lot to your overall productivity. The fundamental reason for using data systems in the first place is to improve business efficiency, which should directly translate to productivity — ensuring that your IT infrastructure operates efficiently and, at its peak, could see a drastic improvement in internal business productivity.

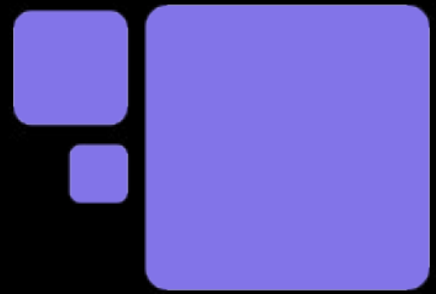
An efficient IT system is less likely to fall victim to cyber-attacks, breakdowns, and downtime, and it also uses less energy and time to complete its tasks. A managed security provider maintains your IT and workplace efficiency by offering security and maintenance services. In addition to all that, outsourcing your IT support and security services frees up your staff to focus on other essential tasks that are better suited to their abilities.

Cybersecurity Assurance

Cybersecurity causes sleepless nights for many entrepreneurs and business leaders. You won't be confident in your security efforts if you're not convinced that your business stands a chance against cyberthreats. A majority of business executives don't clearly understand what they're doing to protect their businesses or whether their security measures even work. This is why you need professional assistance to avoid such well-founded but unnecessary worries.



CHAPTER SIX:
The Takeaway



Rest assured that your data security rests in capable hands by hiring a managed IT security service provider. It's that peace of mind that will empower you to stretch your business even further on the digital landscape and have the courage to explore new opportunities. Don't let fear over cyberthreats hold your business potential back.

It was a long read, and you probably found some of the information in this text a bit overwhelming. The goal of this article was to promote an understanding of cybersecurity and the role of managed security service providers.

In summary, we have established the current state of cybercrime, which is rather shocking and scary. We've also discussed at-length the many different types of threats that every organization should prepare for. And more importantly, we've looked at practical ways of protecting businesses from unscrupulous cybercriminals. It's a lot to take in, especially if you're new to the concept of cybersecurity, but once you break everything down like this, the importance of what we're talking about becomes apparent.

The general takeaway is that all businesses, big and small, need to seriously rethink and re-evaluate their cybersecurity strategies to face up against modern cyberthreats. The repercussions of failing to do so are dire and can easily pull an entire company to the ground. It's really not a gamble worth taking, especially with relatively easy and inexpensive solutions available, such as enlisting the help of an MSSP.

To learn more about managed security services, don't hesitate to get in touch with us. We take pride in helping businesses secure their future by protecting digital resources from modern threats.

**KIRKHAM
IRONTECH**

Kirkham IronTech
3111 Old Greenwood Road
Fort Smith, AR 72903

www.kirkhamirontech.com
479-434-1400