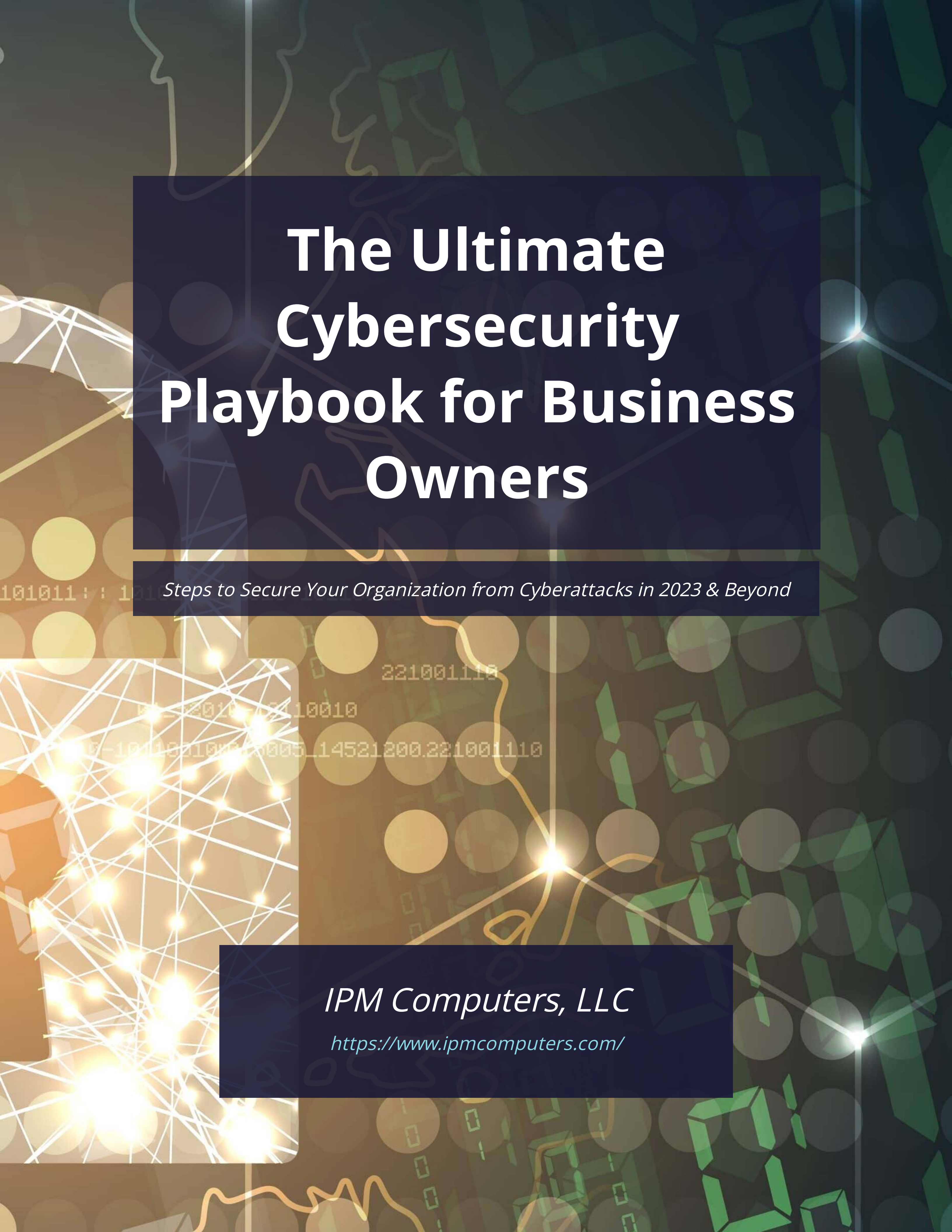


The Ultimate Cybersecurity Playbook for Business Owners

Steps to Secure Your Organization from Cyberattacks in 2023 & Beyond

IPM Computers, LLC

https://www.ipmcomputers.com/

Table Of Contents

01

The Importance of Cybersecurity for Small Businesses

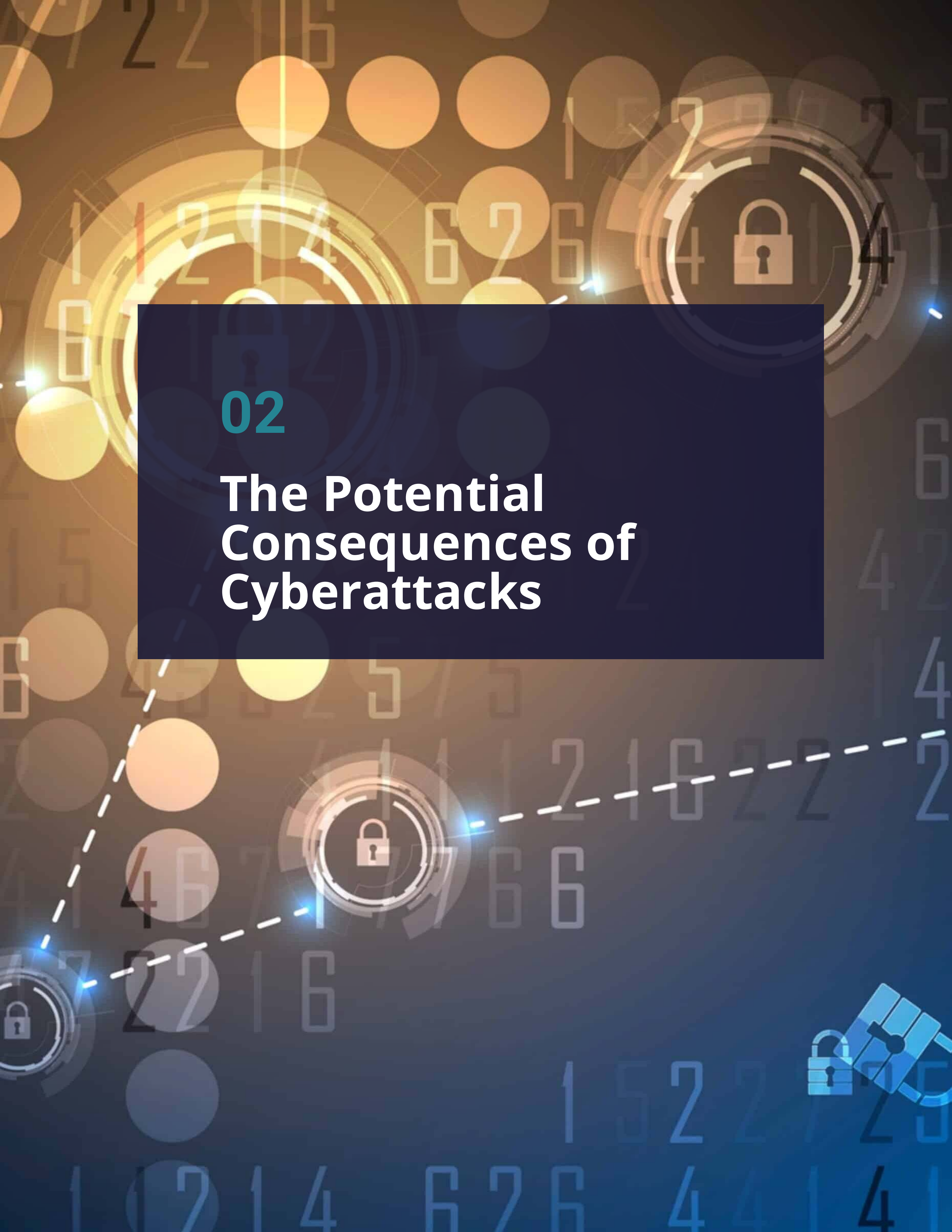
As businesses continue to rely more and more on technology, proper cybersecurity has become more crucial than ever before. Cybercriminals are becoming more sophisticated and constantly looking for new opportunities, so ensuring your business is protected around the clock is essential.

Businesses of all types and sizes are potential targets for hackers. Still, small businesses are often preferred targets because they tend to have weaker security measures. Because of this, businesses of all sizes (even smaller businesses) must take cybersecurity seriously and implement measures to protect themselves.

Have Questions About Cybersecurity?

Are you looking to protect your business from cyber threats? Our team of cybersecurity experts can help. Contact us now to schedule a consultation and gain valuable insight into how we can safeguard your systems and data.

CONTACT IPM COMPUTERS FOR YOUR CYBERSECURITY NEEDS



02

The Potential Consequences of Cyberattacks

The potential consequences of a cyberattack on a small business can be severe. Some of the most common consequences include:

Potential Downtime

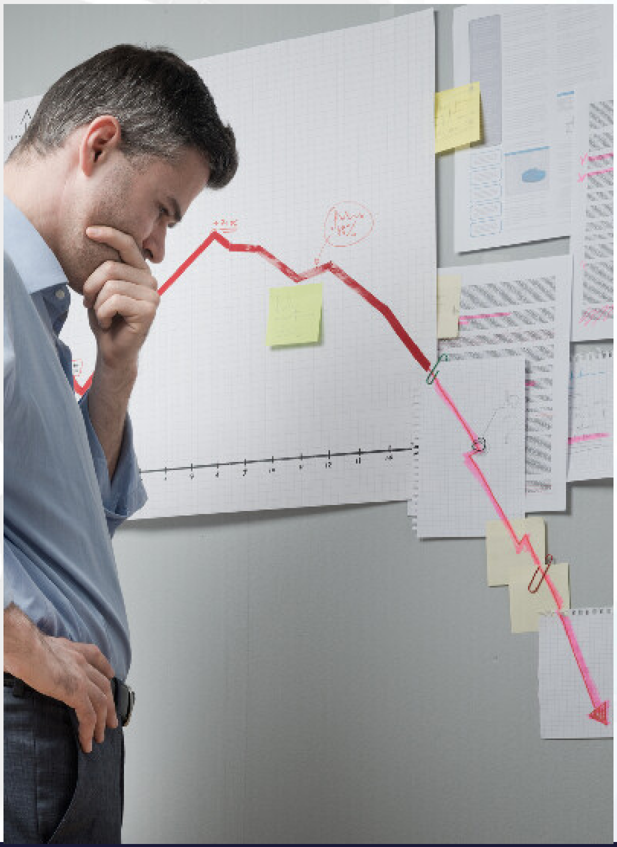
A cyberattack can severely impact an organization's ability to operate. An attack can lead to an inability to access critical systems, such as email and essential software and tools used to run the business, which can disrupt operations and lead to potential financial losses.

Loss of Data

Along with downtime due to losing access to critical software and services, small businesses risk losing valuable intellectual property and customer data during an attack. This can result in losing a competitive advantage and damaging customer trust.

Financial Consequences

A cyberattack can have serious financial consequences due to downtime, data loss (as outlined above), and potential legal issues resulting from an attack. If a business's sensitive financial information is compromised, it can lead to loss of revenue, legal fees, and reputational harm. This can be devastating for a small business that may not have the resources to recover from such an attack.



Protecting Your Business

A successful cyberattack can have far-reaching and long-lasting consequences that can be difficult to recover from, so it’s important to be proactive and take steps to protect your business before an incident occurs.

This may sound like a daunting prospect, but fortunately, there are some simple steps you can take now to improve your company's overall cybersecurity posture. Actions such as enforcing a policy for strong passwords, regularly updating software, educating employees on cybersecurity best practices, and implementing a robust backup and recovery plan can all boost your security.

In the following pages, we'll look at some simple actions you can take today to reduce the chances of becoming a victim of a cybercrime.

Prevent Problems Before They Happen

Don't let a cyberattack bring your business to a halt. Our team of experts can help you secure your business from potential threats and ensure uninterrupted operations. Contact us today for a consultation and keep your business protected.

CONTACT US TO HELP PREVENT CYBERATTACKS

03

Basic Cybersecurity Measures

Basic cybersecurity measures are essential for every business and should be immediately implemented if they are not already. Fortunately, these steps are relatively quick and easy to implement.

Using Strong Passwords

Require your staff to use strong, unique passwords for all accounts. This is one of the simplest and most effective ways to protect against cyber attacks. Using long, complex passwords unique to each account can make it much more difficult for attackers to gain access to your systems.

Enabling Two-Factor Authentication

Two-factor authentication adds an extra layer of security by requiring users to provide a second piece of information, such as a code sent to their phone and their password to log in. This makes it much more difficult for attackers to access your accounts, even if they manage to guess your password.

Regularly Updating Software

Regularly updating and patching software and operating systems is another critical task that should be done frequently. Software and operating system updates often include important security fixes, so keeping your systems up to date is essential. Regularly installing updates and patches can help protect against known vulnerabilities that attackers can exploit.

Implementing a Firewall & Antivirus

Use a firewall to protect against external threats by controlling incoming and outgoing network traffic based on security rules. Using a firewall, you can block or limit access to your network from external sources, which can help prevent attackers from gaining access to your systems.

In today’s post-covid age, many businesses are implementing cloud based firewall solutions. This technology allows remote/mobile employee to remain ‘behind’ a company’s firewall, protecting said employee even when travelling. This also allows IT admins to ensure devices are always connected to the VPN and protected by forcing devices to connect to the VPN automatically.

Anti-virus software has changed dramatically in recent years. Traditional antivirus solutions work by downloading a database of known viurses, and then scanning your computer for any of those viruses. Unfortunately, this is no longer effective in combating mdern attacks. Many viruses today are zero-day-threats, which means they have never been seen before.

Because of this, they would not show up in an antiviruses update, and would not be detected in a scan. To combat zero day threats, businesses need endpoint detection and response software, which utilizes AI and user behavior to detect threats rather than a database. EDR software is usually monitored by a security operations center to ensure 24/7/365 monitoring.

If your organization is currently not doing all of the above, now is the time to act. These actions don't take long to implement, and will make your company much more difficult to successfully attack. Hackers look for easy targets, and ensuring you have these basic cybersecurity measures in place makes your business less appealing.

Need Help With Cybersecurity?

Our team of cybersecurity experts can help implement basic and advanced security measures to protect your business from threats such as phishing, malware, ransomware, and more. Contact us today to learn more about our cybersecurity services and how we can help keep your business safe and secure.

CONTACT US FOR COMPREHENSIVE CYBERSECURITY PROTECTION

04 Email Security

In addition to implementing the basic cybersecurity measures outlined above, you will also want to protect your email systems. Email is one of the most common ways attackers try to access a company's systems and sensitive information. Having the right tools and policies can help harden your overall security.

To protect against email-based threats, implement the following into your business as soon as possible:

Practice Caution

Practice caution regarding email—always double-check emails with links or request sensitive information to ensure they're valid. Encourage your employees to be cautious of suspicious emails and avoid opening attachments or links from unknown sources. Attackers often use email to deliver malicious software, such as viruses and ransomware, to their targets. A vigilant eye will be able to catch these emails and avoid them (some phishing and malicious emails are very well done), so it's important to stay alert.

Use Reputable Services

Use a reputable email security service to filter out spam and malicious emails.

Email security services use advanced algorithms and other techniques to identify and block spam and malicious emails. They will alert users to suspicious and potentially dangerous emails. This can help protect your business from a wide range of email-based threats.

Implement Email Policies

Implement policies and procedures for handling sensitive information via email. Many cyberattacks involve attackers tricking employees into revealing sensitive information, such as passwords or financial data, via email. By implementing policies and procedures for handling sensitive information via email, you can help educate and train your employees to reduce the risk of these attacks.

Protect Your Email Today

Implementing proper security measures and providing your employees with training about sound email safety practices can help thwart a large percentage of cyberattack attempts. If you need assistance implementing a reliable email security solution and adequately training your employees, we can help.

CONTACT IPM COMPUTERS TO SECURE YOUR EMAIL TODAY

05

Network Security

A business network is another tempting target for hackers. Successful attacks on a network can lead to downtime and disruptions, loss of data, and data theft if an attacker can gain entry.

Here are some key steps you should take now to protect against network-based threats:

Secure Your Wi-Fi

By securing your Wi-Fi network with a strong, unique password, you can help prevent unauthorized access. This is especially important if your Wi-Fi network is visible to the public, as attackers may be able to gain access to your systems if your network is not properly secured with a strong, unique password.

Be sure to change your Wi-Fi password as needed. Any time you let an employee go, implementing a new password is a good idea to ensure they no longer have access. This may be a slight inconvenience for in-office staff. Still, keeping your business secure from any potentially malicious actions from an ex-employee is worth the trade-off.

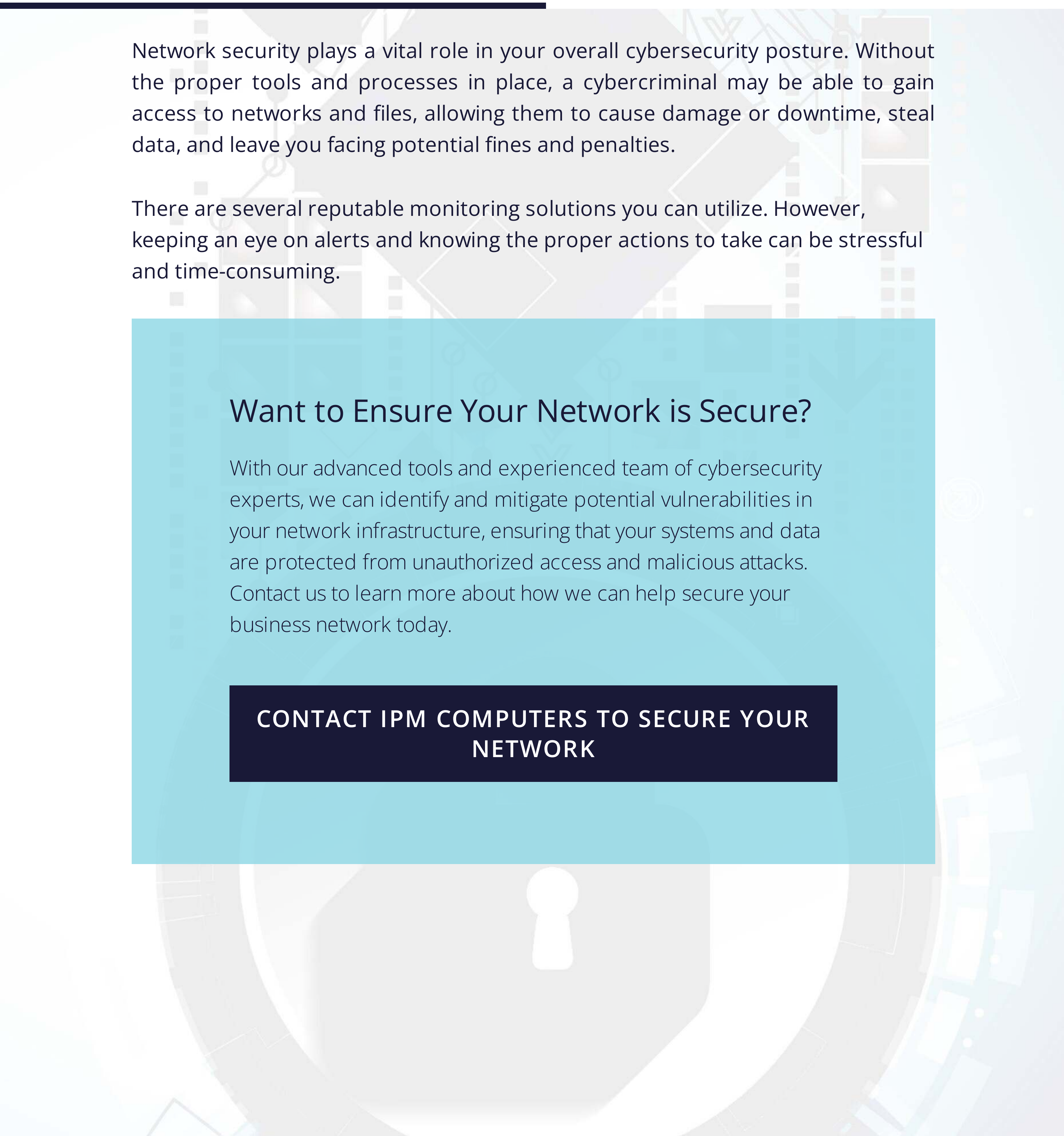
Utilize a VPN

Use a reputable company's virtual private network (VPN) to encrypt your internet connection. A VPN encrypts all traffic between your device and the VPN server, making it much more difficult for attackers to intercept and read your data. This can help protect your business from a wide range of network-based threats.

Ensure that every employee uses this VPN whenever they connect to any business-related services through their devices (whether laptops, smartphones, desktops, etc.). Many services allow you to whitelist IP addresses so that only the authorized IPs can gain access, which can help keep 3rd party attackers at bay.

Monitor Your Network

Regularly monitor your network for unusual activity, such as sudden spikes in traffic or attempts to access restricted resources. Doing so can help you quickly identify potential attacks and take appropriate action to protect your business.



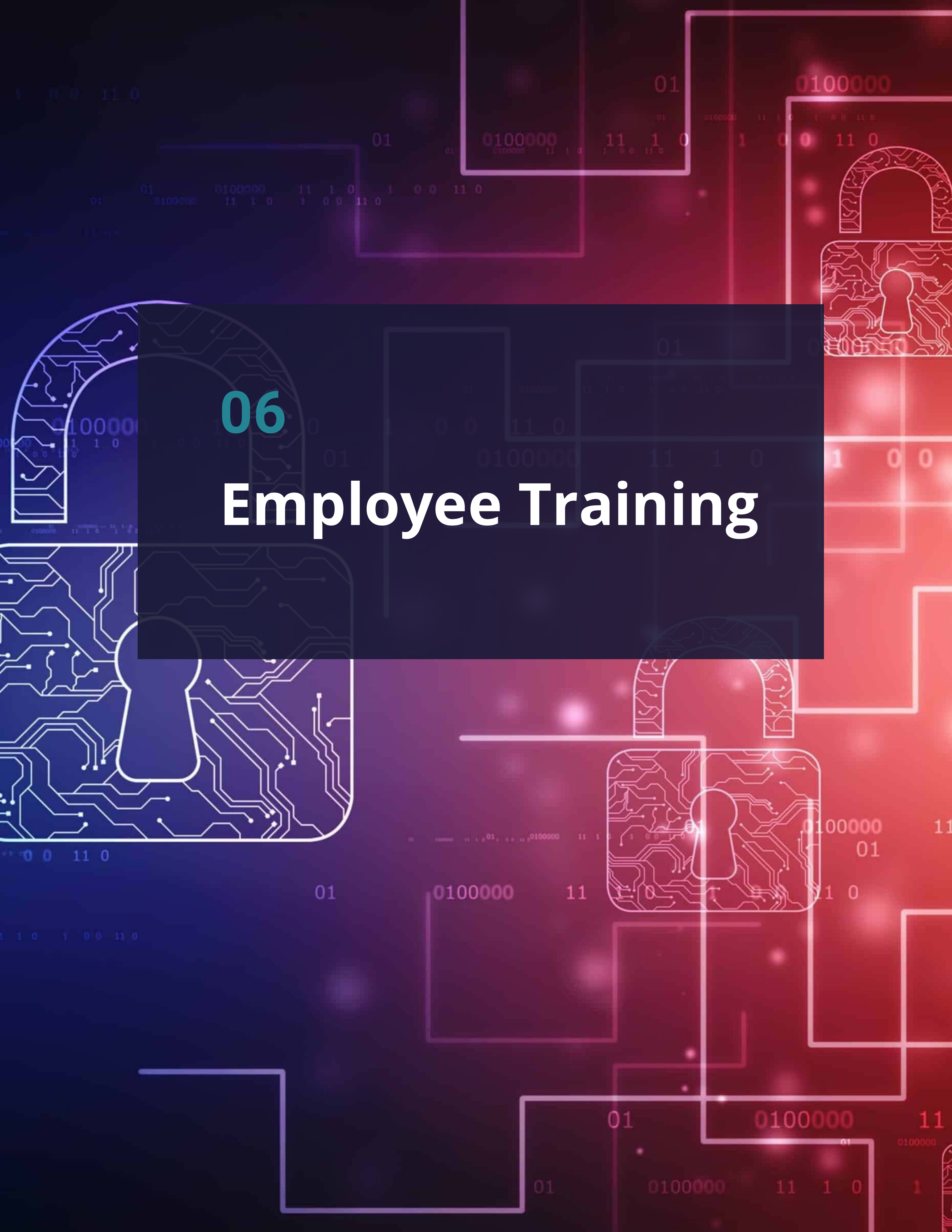
Network security plays a vital role in your overall cybersecurity posture. Without the proper tools and processes in place, a cybercriminal may be able to gain access to networks and files, allowing them to cause damage or downtime, steal data, and leave you facing potential fines and penalties.

There are several reputable monitoring solutions you can utilize. However, keeping an eye on alerts and knowing the proper actions to take can be stressful and time-consuming.

Want to Ensure Your Network is Secure?

With our advanced tools and experienced team of cybersecurity experts, we can identify and mitigate potential vulnerabilities in your network infrastructure, ensuring that your systems and data are protected from unauthorized access and malicious attacks. Contact us to learn more about how we can help secure your business network today.

CONTACT IPM COMPUTERS TO SECURE YOUR NETWORK



06

Employee Training

No matter how good your cybersecurity may be, there's always the human element to consider. An unsuspecting employee may inadvertently provide sensitive information that could be used to compromise a business, so providing them with proper training is crucial. By teaching them to stay vigilant, you can help significantly reduce the chances that they will accidentally grant an attacker the information they need to breach your security.

Here are some simple ways to ensure you provide your employees with the knowledge and systems they need to protect your business:

Educate Your Employees

Educate employees on cybersecurity best practices by providing and requiring regular training on cybersecurity best practices. Doing so can help your employees understand the risks and what they can do to protect your business. This can include strong password management, avoiding suspicious emails, and identifying potential phishing attempts (many topics we've covered so far). Additionally, many cyber insurance poliices are requiring insured entities to provide some form of cyber security training.

Develop & Enforce Policies

As mentioned in the Email Security section of this guide, having policies in place can give your employees the systems and knowledge they need to protect themselves and your company. Develop a cybersecurity policy that outlines the rules and procedures your employees must follow in various scenarios and situations. By ensuring all employees are familiar with these policies through training, you can help them understand their role in protecting your business.

Regularly Remind Your Employees

Regularly remind employees to be cautious when handling sensitive information. Training and policies are key to arming your staff with the knowledge they need to stay secure. Still, these policies will only be remembered if they are routinely revisited. Ensure your employees complete regular training and reviews of your policies to keep them fresh in their minds.

Providing the proper training and implementing policies to help ensure cybersecurity best practices can be a lot of work. Still, doing so is vital as part of your robust cybersecurity strategy.

If you need help getting your employees the training and tools they need to keep your business safe, IPM Computers can help! Contact us to learn more.

Need Help Training Your Employees?

Our employee cybersecurity training program can help your staff understand how to identify and prevent cyber threats, such as phishing and malware attacks. We provide customized training sessions tailored to your business needs. Our experienced instructors will work with your team to ensure they have the knowledge and skills to protect your organization from potential security breaches.

CONTACT US TO GET YOUR EMPLOYEES THE TRAINING THEY NEED

07

Data Backup & Recovery

You never know when a cybercriminal may strike, and there's always a chance that they may attack in a way your company is not prepared to defend against. There's also always a chance that a severe storm or natural disaster may occur that could wipe out your devices, leading to data loss and downtime.

Because of these unknowns, having a reliable data backup solution and a robust recovery plan is crucial to protecting your business. With data backups and a plan in place, you can quickly and efficiently restore access to your systems and data in the event of an attack or data loss.

Perform Regular Data Backups

Regularly backing up important data, such as financial records and customer information, and storing it securely ensures that you always have a copy of this data if it is lost or corrupted due to a cyberattack or natural disaster. While keeping physical copies on external hard drives is a common approach to data backups, doing off-site backups in the cloud is a more robust solution—you can access these files anywhere, they're safe in the event of a natural disaster, and your files aren't stored on physical devices that can be stolen or lost.

Need a Reliable Backup & Recovery Plan?

Don't let unexpected data loss or system failure ruin your business. Our data backup and quick recovery solutions offer reliable protection against data loss and ensure your business is up and running quickly in the event of a disaster.

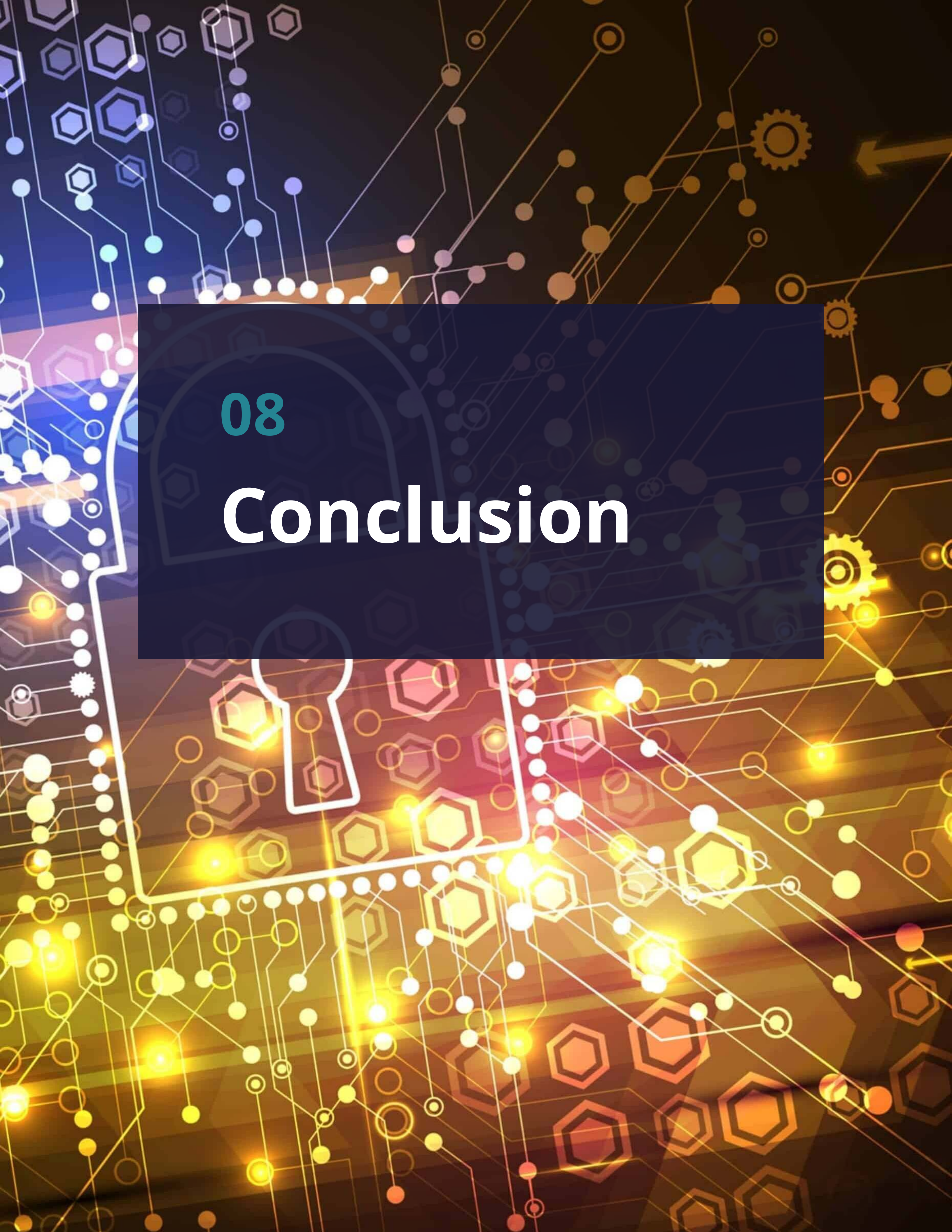
CONTACT IPM COMPUTERS TO SECURE YOUR DATA TODAY

Create a Recovery Plan

In the event of a cyberattack, it is important to have a plan in place to restore access to your systems and data quickly and efficiently so you can keep your business up and running. Creating a robust continuity plan requires a lot of forethought and planning. Still, it's well worth the effort—a well-crafted plan can be the difference between little to no downtime and days (or longer) of downtime.

A robust plan should include aspects such as what to do during an attack (disconnecting devices from the internet, notifying the proper team members, etc.), finding and patching vulnerabilities, ensuring your network is no longer compromised, restoring lost or corrupted data, and notifying the correct people (authorities, impacted clients, etc.).

Implementing a proper backup solution you can rely on can be a lot of work, but it's well worth doing. Similarly, creating a detailed recovery and continuity plan can be a daunting task with many factors to consider, but having a proper plan in place can be crucial in an emergency.



08

Conclusion

Your business, no matter how big or small, needs solid cybersecurity tools and systems in place to protect your company from the ever-growing threat of hackers and cybercriminals.

A cyberattack can have serious financial, legal, and reputational consequences. Your business needs to take steps to defend against these threats.

Basic cybersecurity measures, such as using strong passwords, regularly updating software, and implementing a firewall, can help protect against a wide range of threats. Email and network security are also important, as attackers often use these vectors to access a company's systems.

Employee training is also essential, as attackers often trick employees into revealing sensitive information or clicking on malicious links. Educating and training your employees on cybersecurity best practices can help reduce the risk of these types of attacks.

Finally, having a backup and recovery plan in place is crucial. By regularly backing up your data and having a plan in place to recover from a cyber-attack, you can help ensure that your business can quickly and efficiently restore access to your systems and data in the event of an attack.

Ready to Secure Your Business?

Don't let ever-evolving cyber threats hold your business back. Our comprehensive cybersecurity solutions offer advanced protection for your valuable digital assets. We provide round-the-clock network monitoring and email security to safeguard your business from phishing, malware, and other attacks. In addition, our team of experts can implement robust data backup and recovery solutions, ensuring your business continuity even in the face of a disaster. Contact us now to secure your business and enjoy peace of mind knowing you're safe.

CONTACT IPM COMPUTERS TODAY

Contact IPM Computers for All Your Cybersecurity & Managed IT Needs

As we've seen, there are many aspects to consider when properly protecting your business from cyber threats. Some of the steps outlined above are quick and easy to implement, and you should do so as soon as possible if you haven't already. However, some of these necessary precautions, such as routine updates, monitoring, data backups, and continuity planning, are more significant tasks that will require extra time and effort.

Fortunately, you don’t have to go it alone... IPM Computers is here to help with all your cybersecurity needs. We can help with every aspect of your cybersecurity, from implementing 24/7 monitoring and round-the-clock support to data backups, recovery, and business continuity planning.

We can work with you to create strong policies that better protect your business and help ensure your employees get the training and tools they need to protect your business.

Contact us today at https://www.ipmcomputers.com/ to discuss your security goals. We'll work with you to craft a custom IT plan that fits your budget and exceeds your expectations.