In a world flourishing with technology, new advancements, and cultural adaptations, businesses are now being tasked with protecting their company tech more than ever before.

The Brave River Guide to Cyber Security includes the **15 best security practices** for small to medium sized business to keep your company free of harm.

What acts are you taking to protect your business against this daunting, everchanging struggle?

The best security practices for small to medium sized businesses include:

1. **Create Strong Passwords**
2. **Utilize Multi-Factor Authentication**
3. **Install Anti-Virus Software**
4. **Conduct System Updates**
5. **Start an In-House Security Education Program**
6. **Strengthen Mobile Device Security Policies**
7. **Follow Industry Standards for Compliance**
8. **Implement Physical Methods for Securing Servers**
9. **Test Backup Methods**
10. **Perform Regular IT Maintenance and Backups**
11. **Set up a Firewall**
12. **Conduct Top to Bottom Security Audits**
13. **Social Engineering**
14. **Adapt to New Technologies**
15. **Compile a List of Cybersecurity Necessities**

Create Strong Passwords

Ensure that your business is not threatened from the inside out. Every employee should be creating complex passwords that include both uppercase and lowercase, numbers, and symbols. Passwords such as this make it more difficult for hackers to guess. So long as they are changed every 60-90 days, you'll be smooth sailing with password etiquette.

Utilize Multi-Factor Authentication

Having multiple layers of authentication ensures that only the right people are gaining access to business resources. Having your employees identify themselves through a number of barriers will emphasize the importance of your business' confidentiality.

Install Anti-Virus Software

If your business infrastructure is not backed with an anti-virus software, you are at an incredible risk. Without the proper installation of an anti-malware program, the entirety of your business is jeopardized and could be hacked into. Not only are your business files threatened, but your clients, and employees information is as well.

Conduct System Updates

Don't put off system updates. Be sure to check for updates and complete them when released. New updates will allow your servers, computers, and devices to continue functioning properly and securely—allowing for your business applications to do so as well.

Start an In-House Security Education Program

A one-day PowerPoint presentation just isn't enough anymore. Hackers are getting smarter and savvier; therefore, we need to get together in order to combat this growing threat. Educating your employees on the security policies and procedures will set your business one step ahead of cybercriminals. Stress the importance of these practices and get everyone on the same page about how to keep the business safe.

Strengthen Mobile Device Security Policies

With the rise in mobile devices and on-the-go business, it is critical to determine a policy that extends beyond the four-walls of your company. Creating a standard for mobile cybersecurity can help protect your business, should something happen on or to an employee's device. Simple rules such as having a password protection lock on your device in case of theft, to installing a mobile malware software to your phone—depending on your business, there are a variety of options to implement into your daily practice.

Follow Industry Standards for Compliance

Industry compliance is another aspect to consider when strengthening your security methods. Monitoring any changes and adhering to the regulations set in place by industries, from finance to healthcare, will help keep in compliance with the proper security practices for your field.

Implement Physical Methods for Securing Servers

It takes more than a virtual machine to keep your servers protected. Keeping your servers or other important devices in a protected room with password protection, thumb print, or lock and key are all opportunities to make sure that the physical devices cannot be stolen or damaged.

Test Backup Methods

What's the sense in having a backup if your backup doesn't actually work? Make sure that you run tests to confirm the functionality of your method of backup. Annual backup testing is essential in order for businesses to have peace of mind that their data will be saved if disaster strikes.

Perform Regular IT Maintenance and Backups

Regularly checking on the health of your business infrastructure can protect against a potential downfall. If you didn't bring your car to the mechanic for 10-years, you could be in serious trouble down the road. In addition to maintenance, backing up your data regularly is a positive business practice. By using the Cloud or another personal preference for backups, having an alternative storage space for your information that is up to date will benefit you in the long run.

Set up a Firewall

Don't leave yourself vulnerable to a cyberattack. Your first level for securing your business should be with a strong firewall. With a firewall, you create a barrier between your business and hackers—keeping your confidential information far out of their reach. A firewall will also monitor both inbound and outbound exchanges of information online, detecting any potential intrusions.

Conduct Top to Bottom Security Audits

Top to bottom security audits will examine your business IT infrastructure and devices used to protect it (top), as well as remote or outsourced associate working behaviors and adherence to security protocols (bottom). With technology on the rise, the audit may also include an inspection of automated AI or IoT devices. This process is also known as an edge-to-edge audit, where you inspect the wide range of environments in which security is a factor within your business.

Social Engineering

Through social engineering, your business can begin to minimize human error. Check in regularly to make sure employees are conducting the best security practices and not creating vulnerabilities in your business. From not accessing company files on a public network, to not clicking on suspicious links—creating a culture that places value upon the confidentiality of business resources will help reduce the occurrence of security slip-ups throughout the workplace.

Adapt to New Technologies

Technology is always changing. It is important to move with the times and consider upgrading your methods for security with the release of new means for protection, or even new devices.

Compile a List of Cybersecurity Necessities

Before attempting to implement any of the previous methods for cybersecurity, do consult with your partners or team to consider which avenues might be the best for your particular business. A few things to consider are budget and time. Security may not be cheap, but your business continuity is priceless.

Taking the proper steps to allocate a budget for security as well as maintenance time is critical before diving head first. Not sure where to begin? Brave River is fully equipped with a best-in-class IT Managed Services Team that has the experience, time, and resources to commit your business to a life of safety.

Give us a call today at **401-828-6611** to speak with someone on our IT team and learn about our many IT services.