# 5 Best Practices for Businesses To Follow When Protecting Data Against Cyber Attack

In this presentation, we will discuss the five best practices for businesses to follow when protecting data against cyber attacks. Whether you're a small business or a large corporation, protecting the most sensitive data is important. This not only pertains to your customers but also your employees, your vendors, and others you work with. Failing to protect this data can lead to financial loss, a loss of trust from your customers or clients, a damaged reputation, and, worst of all, legal challenges. So, to avoid all that, please pay close attention to this presentation. Let's get started.

## Implement Strong Access Controls

First, it's always a good idea to ensure that strong access controls are implemented. This is to ensure that not everyone in the business has access to the most sensitive data. For example, consider implementing role-based access control. This will assign permissions based on the employee's role within your organization and allow them access only to the data and systems necessary for their respective roles.

More importantly, you should consider implementing multi-factor authentication (MFA). This requires more than one form of verification for access. In addition to a password, you may also need a fingerprint scan or a code sent to a mobile device. This adds extra layers of security. Finally, review and adjust access privileges regularly to ensure that only authorized individuals have access to sensitive information.

## Keep Software Updated and Patched

Always keep your software up-to-date to defend your computer system against cyber attacks. Outdated software can be vulnerable to exploits and security flaws. For this reason, consider enabling automatic updates whenever possible so updates are installed automatically whenever a new version is available. Also, consider establishing patch management processes to track software versions and apply patches as soon as they become available, even if there is no automatic update.

Finally, conduct regular audits of your software and systems to identify and address potential vulnerabilities. Once these vulnerabilities are identified, it's important to install a recent update or patch to prevent cyber attacks from happening.

## Educate and Train Employees

This step is paramount when running your business. If you have employees, it's important to train and educate them properly on the best cybersecurity practices. Human error is one of the leading causes of cyber incidents, so to mitigate the risk, train employees to identify possible security attacks, such as phishing emails, suspicious links, and other threats.

Perform simulated phishing exercises to test employees' ability to identify and respond appropriately. Any potential situations where a cyber attack may occur should be reported. Create an environment where employees feel comfortable reporting any potential threats or suspicious activities.

## Implement a Data Backup and Recovery Plan

Backing up your business data regularly is crucial. Having a backup handy, even after a cybersecurity attack, ensures that your business can recover quickly. In addition to regular backups, test recovery procedures so you and your employees are better prepared for incidents such as cyber-attacks, natural disasters, or power outages.

Finally, familiarize yourself with data retention policies that will allow you to keep data for as long as necessary. This reduces the risk of exposure and ensures you have sufficient space to handle more data in the future. Don't forget that retention policies may also be tied to regulations you must follow.

## Monitor and Respond to Threats

Last but not least, be proactive in monitoring for any unusual or suspicious activity and respond to threats accordingly. Utilize tools that monitor your network for any unusual activity. Implement an intrusion detection system to detect and mitigate any potential attacks in real-time. Consider installing an incident response plan to address a cyberattack should one arise. Continue improving your business's computer system and regularly update your incident response plan to adapt to new threats while enhancing your overall security posture.

## Final Thoughts

We hope your business follows these five best practices for protecting data against cyber attacks. Not only is it highly recommended that you do so, but there may be regulations based on your industry that require you to follow these practices. We hope this presentation was informative for you. Thank you for taking part, and make sure your business stays safe.