# Cyber-Incident-Prevention Best Practices for Your Small Business

Did you know that small businesses like yours are just as vulnerable to cybersecurity threats as large companies? Only 5% of small business owners think cyberthreats are the biggest risk to their business today.[1] Unfortunately, it's a myth that cybercriminals are more interested in stealing data from large enterprises. In fact, cybercriminals expect small businesses to have less security measures in place, making it easier for them to get what they want.

If you experience a data breach, bringing systems back online and restoring data can be a huge challenge. On top of that, you'll need to notify all affected clients that their data may have been compromised. That's a tough position no small business owner wants to be in.

By taking proactive steps for cyber incident prevention, you can dedicate more resources towards growing your business and avoid experiencing cyber incidents.

Z-JAK Technologies

# TOP
# Cyber-Incident-Prevention Best Practices

- **Provide cybersecurity training for your employees:** Your company is more secure if your employees are constantly trained on cybersecurity best practices. By educating your workforce on various cybersecurity risks, from data theft to ransomware, you can prevent them from committing simple errors.

- **Stay up to date with software patches:** If you're running on operating systems and applications that aren't updated frequently, you're exposing your business to countless vulnerabilities. Unpatched applications can serve as a gateway for attacks. The best way to prevent malware from infecting your computer is to patch your system and applications.

- **Enable multifactor authentication to safeguard accounts:** With the addition of two-factor authentication, a hacker will have a much more difficult time gaining access to your online accounts. This is one of the easiest and least intrusive ways to add security to your accounts.

  By providing additional barriers that thwart malicious actors, multifactor authentication maintains the security of your data and systems. It's highly improbable that a hacker will have an additional authentication factor, even if a password or other login technique is exploited.

- **Require employees to work on a Virtual Private Network (VPN):** VPNs are used to protect and maintain the privacy of your company's network. Hackers won't be able to see what pages your employees visit, the passwords they use or any sensitive data they access because VPNs encrypt their online activities.

- **Encrypt your data:** With encryption, you can keep your business data hidden from unauthorized users, preventing them from accessing private information and sensitive data while enhancing the security of communication between client apps and servers.

- **Have a backup of sensitive data:** Proactive data backup methods can increase security for your company and give you the ability to address any unanticipated data loss circumstances while ensuring business continuity. Creating backups is an excellent way to start because data loss can occur at any time and in a variety of ways.

What happens if you experience a cyber incident despite taking every precautionary measure? To respond to the issue quickly and lessen its impact on your company, you must have an incident response plan in place.

Z-JAK Technologies

# 5 KEY PHASES
## of NIST's Incident Response Framework

**1** **Identify:** If you want to manage your cybersecurity risk, you need to have a comprehensive understanding of your tech environment. This function requires a company to have visibility over its digital and physical assets, clearly define its roles and responsibilities, identify the risks it faces, and create policies and procedures to manage those risks.

**2** **Protect:** Your IT service provider should keep track of both digital and physical resources, provide awareness and training, safeguard data, and oversee network configuration baselines and operations during this phase of the incident response framework. This will guarantee that compromised system components are quickly rectified. To increase cyber resilience, you should also implement preventive technology.

**3** **Detect:** To swiftly identify cybersecurity incidents, your business must take proper measures. You need to constantly monitor systems that recognize unusual activity and other risks to your operational continuity. It is imperative for a business to have full visibility into its networks so it can anticipate a cyberthreat and act appropriately in the event of one. The best way to detect and prevent cyberattacks on ICS networks is through constant surveillance and monitoring of threats.

**4** **Recover:** Getting your affected systems back online following an attack or incident is the focus of the recovery phase in your incident response plan. This will depend on whether the systems' flaws have been fixed and how your company plans to make sure they aren't exploited again.

During this phase, your affected systems are tested, monitored and verified. If you fail to ensure adequate recovery, you can have difficulty preventing another similar disaster in the future. We all know how terrible that can be for operations and your reputation.

**5** **Respond:** When your business experiences a cyber incident, you need to develop a response strategy, pinpoint channels of communication between the pertinent parties, gather and analyze case data, carry out all necessary actions to put an end to the incident and incorporate any lessons gained into updated response tactics.

As the frequency and complexity of cyberthreats continue to grow and evolve, you can protect your business by partnering with an IT service provider.

An IT service provider like us can prepare your organization for a variety of cyber incidents, including ransomware attacks, phishing scams, data loss and technical difficulties. When you have an incident response plan in place, you can limit the damage caused by these incidents while also giving your employees an action plan to follow.

***Contact us today to get started on your incident response plan.***

**References:** [1]CNBC | SurveyMonkey Small Business Survey, 2022

**Z-JAK Technologies**
**www.zjak.net**
**info@zjak.net**
**(502) 200-1169**