Exceptional Home & Business
Technology Solutions

IT Support, Managed Services, Networks, Servers, Computers, VOIP Phone Systems
since 2004 with locations in Lockport, IL and Bonita Springs, FL

JK CONSULTING

Does your business have a cyber readiness plan?

With headlines full of cyberattacks and security breach victims, it is time to take the risks seriously. The success and survival of your business will be determined by your ability to overcome security threats or breaches. You need a cyber readiness plan that includes elements of prevention, continuity and recovery strategies.

Average Ransom Paid in 2020 $5,600

Average Downtime Cost in 2020 $274,200

Ransomware attacks can result in considerable business downtime, because breaches are rarely limited to a single computer. Most of the ransomware in use today is designed to crawl business networks, looking for additional machines to infect. If the malware goes undetected, it doesn't take long for numerous user devices, servers, and even data in SaaS applications to become encrypted. Restores can be time consuming, especially using traditional backup tools.

#2 Establish Strict Policies and Procedures

Have you defined the rules and protocols for security in your business? Policies and procedures regulate business operations and are essential for defining the standards and expectations of employee behavior and actions in the workplace.

While establishing strict, security focused protocols is essential, a system of validation and enforcement is equally important. After all, rules without consequences are merely suggestions. Let us help you develop security-driven policies and procedures for your business.

#3 Keep Updates Up to Date

Does your organization have any missing security updates?
While updates often introduce new or enhanced features into your apps, programs and systems, they also install security and performance fixes known as patches. Undiscovered defects or flaws can leave your systems exposed. Hackers will exploit any vulnerability or security gap they find. Keeping your systems updated is vital for keeping your business cyber ready.

Does your business have a cyber readiness plan?

#4 Force Authentication

Secure your business from cyber threats and bad actors by enforcing multi-factor authentication.

One-level security is no longer enough. Even the strongest passwords are vulnerable to theft or exposure. Requiring more than one method to authenticate user identity or access permissions can reduce or eliminate the risk of stolen or unauthorized credentials being utilized.

#5 Back Up Everything

What are you doing to protect and preserve your organization's data and its accessibility?

Data is the lifeblood of every business. Unfortunately, the risks and threats to the protection, privacy and usability of that data are endless.

Follow the 3-2-1 method for backups; a minimum of three unique copies of your data, two available locally and one off-site or in the cloud. Make sure to test your backups often for functionality and integrity.

Ensure that your data is protected and secure from cyber threats.

#6 Don't Neglect Compliance

Maintaining regulatory compliance is mandatory for many organizations. While navigating and satisfying the obligations can be complicated and stressful, achieving compliance is a critical component of having a cyber ready business. Security and privacy are integral elements of compliance, Let us take the stress out of compliance for your business.

Does your business have a cyber readiness plan?

#7 Continuous Network Intelligence

Do you have on-demand insight into suspicious activity, changes or threats on your network? Knowledge is power. A critical component of cyber readiness is having on-demand insight of anomalous activities, suspicious changes, potentially harmful misconfigurations or any other malicious activities occurring internally on your network. Promptly detect and remove threats before they cause damage.

#8 Security Awareness Training

Users are the weak link in security given a lack of education and experience. Are you training your team to recognize threats?

Instituting a security awareness training program for every member of your staff will significantly reduce the probability of user-related errors and exposures.

#9 Combat the Password Crisis

Is your organization guilty of sacrificing security for convenience when it comes to passwords?

With over 80% of hacking-related breaches linked to weak, reused or stolen passwords, user credentials are emerging as the top vulnerability for businesses.

Balance convenience and security by monitoring the dark web for exposed credentials, implementing multi-factor authentication, and streamlining control of password management.

Does your business have a cyber readiness plan?

#10 Don't Skip the Insurance

Is your business covered by the correct policy should the worst occur?

Increasing risks and threats of data breaches and ransomware, regardless of size or industry, have prompted many businesses to adopt Cyber Risk Insurance to protect themselves from catastrophic loss. Investing in a cyber insurance policy could save your business should you be the next victim.

#11 Reduce Supply Chain vulnerabilities

Don't let security incidents from your supply chain become headaches for your organization.

Nearly two-thirds of firms (65%) have experienced cyber-related issues in their supply chain in the past year.

As a part of your cyber readiness plan, you must deploy protocols to evaluate and monitor the security of your supplier networks and third-party vendors.

#12 Deploy a Multi-Layer Security Strategy

Nothing is failproof. Is your company taking advantage of all the security protections possible?

Security is asymmetrical. Where businesses must plan, prepare and defend against every threat or scenario, cybercriminals only need to find a single weakness or hole in your defenses to carry out their malicious plans. Protect your data and your business by deploying multiple security strategies together as one.

Let JK Consulting help you develop and apply a defense in depth approach.