IT Support, Computers, IT Networks, Managed Services, VOIP Phone Systems

Cybersecurity Solutions

Keeping Your Data Safe

Supporting your technology needs since 2004 with locations in Lockport, IL and Bonita Springs, FL

Cybersecurity Is Your Company Protected?

At JK Consulting Cybersecurity is serious business. Network security and loss of data are a constant threat to your bottom line. One single data breach or ransomware attack can cost your business tens of thousands of dollars. Internal and external security threats must be considered seriously. JK Consulting will develop a detailed security plan that covers your network and all endpoints. We will provide consistent security support and peace of mind that your IT infrastructure is sufficiently monitored and secured.

What is Cybersecurity?

Cybersecurity – the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access – is a popular topic in government and corporate circles, and is a growing concern for smaller businesses.

The JK Consulting 7 Step Plan to Cybersecurity

1) Cybersecurity Training Program
2) Antivirus Software
3) Advanced Firewalls
4) Software Patch Management
5) Password Management
6) Backup and Recovery
7) IT Compliance

Security & Peace of Mind

In an era of the ever-evolving security landscape, small-and medium-sized businesses (SMB's) face large challenges when it comes to defending their networks, data and reputation. Keeping up with changes in technology can be as difficult as tracking the growing number of threats.

JK Consulting North 988 E 9th Street, Lockport, IL 60441 815-588-4530
JK Consulting South 24860 S. Tamiami Trail, Suite 1, Bonita Springs, FL 34134 239-294-8217
www.jkconsulting.com

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

2020 stands apart as a year where the entire world shared a crisis unparalleled in recent memory. Technology infrastructure was tested to the limit by companies large and small as they built their "new normal". Cybersecurity continues to hold a high position of importance among Small and Medium Businesses (SMB's). In a recent survey of 700 SMB's conducted by independent technology market research specialist Vanson Bourne some very interesting data was revealed.

86% of SMB's report cybersecurity to be within the top five priorities for their organization and 38% say it is their top priority.

77% of SMB's worry they will be the target of an attack in the next 6 months.

73% of SMB's are planning to invest more or much more in cybersecurity in the next 12 months.

60% of SMB's will invest more in cybersecurity because it reduces risk for their organization.

57% of SMB's do not have specific cybersecurity experts in their organization.

52% of SMB's agree they lack the in-house skills necessary to properly deal with security issues.

The Impact of Security Incidents on SMBs

In another survey conducted by the Better Business Bureau of Small and Medium Businesses (SMB's) cybersecurity continues to be at the top of the list for nearly every participant. That perhaps explains why over three quarters are worried they will be the target of an attack in the next 6 months. 55% of SMB's have reported suffering a cyber attack, and the impact is considerable. The average cost of an attack has grown from last year, when it stood at $50,865, compared to this year where it has risen to $58,902—an increase of nearly 16%. And the larger the size of the SMB, the more significant this cost becomes.

Have You Heard Of Any Of The Following Risks To Your Organization's Cybersecurity?

RANSOMWARE: Scammers breach the operating system and download a type of malicious software designed to block access to a computer system or hold data hostage until a sum of money is paid.

PHISHING: Communication impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the business into providing sensitive information or passwords.

POINT-OF-SALE MALWARE: Specialized malware loaded onto point-of-sale devices that remotely captures data from each card swiped at that cash register.

KEYLOGGERS: Hardware or software that captures each keystroke on a device and makes it available to an attacker.

TECH SUPPORT PHONE SCAM: Scammers pose as a security monitoring service that has (falsely) detected a virus on your computer. Often, they then charge you to install software to clean it up. This software actually gives them remote access to your computer.

REMOTE ACCESS TROJAN or RAT: Malware that connects to an attacker’s server and provides complete access to the infected machine including keyboard, screen, webcam, and files.

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

The 7 Lines of Defense of JK Consulting Will Implement.

1) Cybersecurity Training Program

The importance of providing regular, evolving security & phishing awareness training cannot be overstated. 90% of incidents that end in a data breach start with a phishing email. Continually educating staffers about potential security threats ensures that they're ready to spot and stop potential phishing attacks – providing peace of mind, shoring up security, fulfilling cybersecurity best practices, and ensuring greater data privacy compliance. JK Consulting provides thorough phishing resistance training in bite-size pieces, making employees more likely to retain what they learn and avoid phishing dangers.

2) Antivirus Software

Cybersecurity technology starts with antivirus software. Antivirus, as its name implies, is designed to detect, block, and remove viruses and malware. Modern antivirus software can protect against ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, adware, and spyware. Some products are designed to detect other threats, such as malicious URLs, phishing attacks, social engineering techniques, identity theft, and distributed denial-of-service (DDoS) attacks.

3) Advanced Firewalls

A network firewall is also essential. Firewalls are designed to monitor incoming and outgoing network traffic based on a set of configurable rules–separating your secure internal network from the Internet, which is not considered secure. Firewalls are typically deployed as an appliance on your network and in many cases offer additional functionality, such as virtual private network (VPN) for remote workers.

4) Software Patch Management

Patch management is an important consideration as well. Cyber criminals design their attacks around vulnerabilities in popular software products such as Microsoft Office or Adobe Flash Player. As vulnerabilities are exploited, software vendors issue updates to address them. As such, using outdated versions of software products can expose your business to security risks. There are a variety of solutions available that can automate patch management.

5) Password Management

Recent studies have reported that weak passwords are at the heart of the rise in cyber theft, causing 76% of data breaches. To mitigate this risk, businesses should adopt password management solutions for all employees. Many people have a document that contains all of their password information in one easily accessible file—this is unsafe and unnecessary. There are many password management apps available today. These tools allow users keep track of all your passwords, and if any of your accounts are compromised you can change all of your passwords quickly.

Encryption is also an important consideration. Encrypting hard drives ensures that data will be completely inaccessible, for example if a laptop is stolen.

6) Backup and Recovery

Taking frequent backups of all data considered vital to your business is critical. The exact frequency of backups will vary based on your business' specific needs. Traditionally, most businesses took a daily backup, and for some businesses this may still be suitable. However, today's backup products are designed to make incremental copies of data throughout the day to minimize data loss. When it comes to protecting against cyber attacks, solutions that back up regularly allow you to restore data to a point in time before the breach occurred without losing all of the data created since the previous night's backup.

7) IT Compliance

IT Compliance is taking appropriate control of and protecting information, including how it is obtained and stored, how it is secured, its availability (how it is distributed internally and externally), and how the data is protected. The internal compliance functions revolve around the policies, goals, and organizational structure of the business. External considerations include satisfying the customer/end user while protecting the company and end user from harm. Specialized tools are used to continuously identify, monitor, report, and audit to achieve and remain in compliance.