12 IT Best Practices

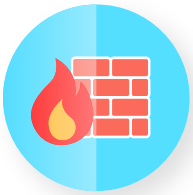
for a secure and productive business

1 Antivirus

Install antivirus software on every server and workstation. If you use an internal email server such as Microsoft Exchange Server, you should also protect your email messages with antivirus.

The most effective management of antivirus scans, virus definition update and threat management is achieved with a network version of antivirus that is managed by a central server. It is also important to exclude certain files and folders from virus scanning due to the possibility of data corruption. This is particularly important on servers such as Domain Controllers, Exchange Servers and Database Servers.

2 Internet Security

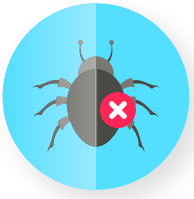


It is a necessity for most businesses to be connected to the Internet in order to conduct business. This connection is an often overlooked security risk. Without the proper hardware in place, the information stored on your network can be accessed by unauthorized persons.

There are three types of hackers: The one who wants to retrieve data for personal or resale use, the one who wants to be destructive within a vulnerable network, and the one that wants to take control of your network computers in order to send spam, attack other companies or hold your data for ransom. Whatever the motive, the results can be catastrophic and expensive. The solution is a **firewall appliance.**

3 Malware Management

Malware is a broad term that refers to software designed to infiltrate or damage a computer system without the owner's consent. Popular forms of malware include spyware, adware and ransomware. These programs are responsible for a significant decrease in user productivity due to their impact on PC performance and time spent on attempted self-repair.



The solution is to proactively scan for and remove malware programs on a regular basis by a qualified PC administrator using utilities designed for the task.

4 Junk Email

Spam isn't just a can of mystery meat anymore. Spam is Internet slang for unwanted email. Spam is an intrusion that can become a financial drain by impacting the productivity of users, the performance of computers, and the speed of Internet access because of a "clogged drain."

Spam has also been linked with fraudulent business schemes, chain letters, and offensive sexual, political, hateful, or other inappropriate messages that may violate the company's workplace or computer-use policies. Spam is also a favorite delivery method of viruses and other malware like spyware, adware and ransomware.

The solution is to subscribe to an inexpensive cloud service or install hardware or software that filters this content before it gets delivered to your Inbox. Business users of the Microsoft Office 365 system have access to the same services as part of their cloud subscription.

Worried about missing emails? Most services let you view your own private quarantine so that you can release anything that was improperly categorized as spam. They will also provide the option of always allowing the sender or domain through in the future. This is referred to as a "white list".

One more bit of caution: If you ever find that your organization is unable to send email to common recipients, make sure that your domain name has not been inadvertently added to a "black list" as a source of SPAM. It happens often if your organization sends electronic newsletters or other mass emails.

5 Data Backup

Your business should have a data backup solution. Data can be lost in a number of different ways,including: hard drive failure, database corruption, virus activity, end-user error, natural or man-made disaster or an Internet attack by unauthorized personnel.

The value of data varies widely by organization, but could result in an unrecoverable loss of revenue, or even business failure. Methods available for data backup include: rewritable CDs and DVDs, external hard drives, online storage services, remote offsite data transfers, or the traditional antiquated method of automated backup to tape media.

Regardless of the method, it is a best practice to rotate data backups to a safe offsite location, and to perform at least a semi-annual restoration and disaster recovery simulation to test your solution.

6 Microsoft Updates

Disable automatic installation of Windows Updates on servers. Updates can cause unexpected results, including server failure, which can be difficult to diagnose and/or reverse. Instead, consult with BizTech on a regular basis to perform managed updates.

You should enable Automatic Updates on computer workstations, though, as frequent security updates are released by Microsoft.

7 Remote Access

Many organizations operate outside the traditional four walls of the office space. Secure, remote access to corporate environments from remote locations is a necessity.

Remote access serves a number of different needs including: working from home, corporate network access for a traveling sales force, connecting branch offices, accessing servers or individual office PCs, and access for technicians to quickly diagnose and resolve most computer-related issues without the additional expenses related to time traveling to the client's location.

It is important to understand the risks that go along with providing remote access. Proper precautions must be taken to minimize the possibility of unauthorized access. Implementing and enforcing a strong password policy is a good first step. Passwords with a **minimum** of eight characters, using numbers, upper and lowercase letters, and even symbols can increase security. Additional steps such as encryption and biometric user identification can substantially increase security.

8 Server Virtualization

Server Virtualization is the process of creating a virtual, rather than physical server. Software simulates the physical server, and allows your business to run multiple operating systems and applications on a single physical server at the same time. This results in increased IT productivity, efficiency, and agility and responsiveness.

Converting your physical servers to virtual servers (P2V) is commonly used to relieve your business' dependence on your physical servers which are at the end of their life expectancy, but are still able to meet your continuing business needs. Doing so can save your organization a bit of money by getting more life out of your existing servers.

You can use a virtual server to reduce downtime, save on energy costs, reduce system admin work, extend the life of older applications, increase scalability and portability, and help move your business to the cloud. Virtualization is the basis for cloud computing.

9 Cloud Computing

The cloud is not a place or a thing, but is something that every business, no matter how big or small, should get on board with.

Cloud Computing is the delivery of computing as a service, rather than a product, whereby shared resources, software and information are provided to computers and other devices as a utility (like the electricity grid) over a network (the internet). As consumers of electronic devices, we all use cloud services. There are many benefits common to virtualization and cloud based services, including:

- **Reduced Costs** - Upfront and ongoing hardware, software & licensing costs are reduced, as you don't need to purchase servers and other equipment. With many cloud services, you only pay for what you need or use. Another bonus is decreased energy costs.
- **Increased Efficiency** - You can access your files anytime, anywhere, using any device. Files are no longer stuck on one computer or server. Also, cloud services are maintained and updated regularly, so you spend less time doing IT Admin tasks.
- **Easy Collaboration** - Saving and accessing files through the cloud allows everyone to work from the same master document.
- **Disaster Recovery** - If an employee loses a laptop or other device, or if there is an event that causes your business to lose your data, it is fast and easy to recover if you use cloud data backup.

10 Hardware Lifecycle Management

Most companies have equipment at various levels of age and capability. Replacing the vital parts of the IT infrastructure at predefined intervals can provide maximum resource availability, new features, and improved performance.

Servers and other enterprise-level network equipment are designed to be operational around the clock for many years. Most equipment will continue to run beyond their decommission date, but replacing the most critical equipment before it fails allows for thorough evaluation, planning, and testing, which makes for an easier transition to new hardware.

11 Printer Maintenance

One area of IT that many people often overlook is printer maintenance. Regular maintenance of printers and copiers can maximize availability and print quality.

The maintenance interval is dependent primarily on the printer's workload and operating environment. Heavily-utilized printers and those in a harsh environment require more frequent care and cleaning.

12 Consult with a Microsoft Partner

Make sure to consult with a qualified Microsoft Partner before adopting any new Microsoft products for your business. Despite the media excitement over new product releases, it is important to understand what the impact will be in your work environment.

For example, there are still a sizeable number of devices and applications which are not compatible with the latest Operating System, Microsoft Windows 10, which is available in several different versions (some of which are not intended for use in a corporate environment, and cannot be joined to a corporate network).

Microsoft Office 2016 (and Microsoft Office 365), are examples of newer products that can have a significant impact on your business operations because they cannot be installed on systems running older versions of Microsoft Windows; and older Microsoft Office versions cannot open documents created by these new versions without downloading a Compatibility Viewer.

As a result, customers may not be able to read the documents you send unless you saved the file in a backwards-compatibility format, or they apply the compatibility viewer download. One concern is Microsoft Outlook 2016, which includes a new server communications protocol that is not supported on older version of Microsoft Exchange Server.

BizTech

@ 419.539.6922

www.gobiztech.com