

THE HAWK I VIEW



Hawk iSolutions Group, Inc.

What's
Inside

If Disaster Strikes, Is Your Company Safe?

Hurricane Katrina Is A Grim Reminder

You hear it all the time from us—back up your data, keep your virus protection current, and install and maintain a firewall to protect yourself from hackers and other online threats.

However, with the recent and horrible devastations that hurricane Katrina created for businesses and home owners alike, you can see that anti-virus software isn't enough to protect your technology investments or your company's critical data and records; that is why natural disasters also need to be taken into consideration when writing your company's disaster recovery plan.

Do You Have A Disaster Recovery Plan?

We all know that an ounce of prevention is worth a pound of cure; yet, disaster recovery planning often takes a distant second to the daily deadlines and pressures of running a business. According to a recent survey commissioned by AT&T, about one-third of 1,200 respondents said they have no business continuity plan in place. Of those who do, nearly a quarter of the companies surveyed said they hadn't updated their plans in the past 12 months, and nearly as many hadn't tested them during that time either.

That means that most businesses, including your own, may be completely vulnerable to even a bad lightening storm. Studies have also shown that most companies do not recover from a major catastrophe that involves loss of company data. Here's something else to consider if you think that you don't need a disaster recovery plan for your business: "natural disasters" can also take the form of office fires or terrorist attacks, not just storms, earthquakes, floods and tornados. If an electrical problem caused a fire in your building, the parts that weren't burned beyond recovery would probably be destroyed by the firemen's efforts. Another common disaster is damage caused by ruptured water pipes.

If Katrina has you re-thinking your own disaster

recovery plan or wondering what you would do in the same situation, you should take action and start protecting yourself now. The following tips will help get you started in the right direction.

Disaster Recovery Questions You Need To Answer

Most business owners shy away from creating a disaster recovery plan because they don't know where to start, or because they think it will cost them a lot of time and money. For large financial institutions or companies maintaining mission critical data or software, this may be true; however, most small and mid-size businesses only need to take a few precautionary steps to ensure their businesses will continue running in the event of a natural disaster. First, ask yourself the following questions...

1. Do you back up your company's data daily?
2. Do you keep a copy of your back up off site?
3. Would you have access to your data remotely if you couldn't get to the office?
4. Do you know how long it will take the IT department to retrieve a server back up? In many cases it takes days and often weeks; what would you do during that period of time?
5. Do you regularly test your back up system to make sure it is a good copy and not corrupted?
6. Do you store critical program passwords in a secure place that company officers can access if you are unavailable?
7. Do you have a UPS (uninterruptible power supply) device in place to keep your network and other critical data operations running during a power outage?

These are just a few of the questions you need to answer. Obviously, other issues like insurance coverage and operational plans should also be integral elements of your plan.

**Find Out If
Your
Company
Will
Survive If The
Computer
Expert Ever
Quits?**

**Continued
from Last
Month,
Securing
Your
Wireless
Network**

**Quick Tip :
How To
Add A
Shortcut**

**Beware:
"Fun"
Web Surveys**





Are You Doomed If Your In-House Computer Expert Quits?

Here's an important question that most small business owners don't know how to answer: what would happen if you suddenly lost your in-house computer expert?

Most small business owners believe if they lost that expert nothing important could go wrong. In fact, the opposite is usually true. Most small businesses have someone who holds the keys to their entire network; if that person unexpectedly departs as this could be an illness, death, vacation, as well as quits, it could end up costing them time and money and could have a serious impact on the security and operation of the business. Want to know how much it would impact your company? Ask yourself the following questions:

1. Do you know all the passwords?

Every machine and internet related device on your network has (or should have) a password. If you don't know what they are, you cannot view, change, or update the system settings. You should also know the password to your company database and accounting package.

I highly recommend maintaining a password list that is updated whenever a new password is added or changed. Your technician might already have this list, but might not be sharing it with you. Check with them about obtaining a copy of all the passwords to your network and establish a system for obtaining updates.

2. Do you know where your backup files are stored, and if they are being stored properly?

Backing up your data is like brushing your teeth; it's boring, monotonous work, but it must be done every day. If you are like most business owners, you're too busy dealing with the "crisis of the day" to think about system backups and probably leave tasks to your internal expert. If your database gets fried and your tech is no where to be found, you might be in a lot of trouble. In fact, not only should you make sure your backups are being done regularly, but you should also check that they are being done right. The absolute worst time to check the accuracy and reliability of your back up system is in a crisis situation. It's not uncommon for a backup system to become corrupt from an overload of data or a user mistake. If this happens, it could *appear* that your network is being backed up, even though it's not. Our recommendation: Perform a restore. As you know, the objective is not to "backup" a system; the objective is to "restore" a system. Give us a call if you would like for Hawk iSolutions Group, Inc. test your backups.

3. Do you have all the product keys to your software?

Product keys are long, alphanumeric codes, usually printed on the back of the software's packing material, that are required to install the software. Once installed, you don't need them again...UNLESS your system becomes unstable and you need to reinstall the program.

4. Do you know where all the software disks are stored?

As a follow-on to the above question, you should also know where all of your software disks are stored. Bad things happen to computers, and the situation can be made worse if you are not prepared. Taking a minute to organize and store your software disks in a secure place can save you a considerable chunk of money in the event that you need to restore a program on your computer. If you don't have the disk, you might be forced to buy the software again.

5. Do you know what routine maintenance must be done to your network?

I know that the very idea of learning about and keeping track of all the servers, workstations, and peripherals on your network probably gives you a major headache, but it is important information to maintain. If your in-house expert leaves, who will take over? Although it isn't rocket science, it is very important to know what maintenance is required and when. Learn about and understand backups, database maintenance, system updates, security patches, virus updates, system resets, and more.

6. Do you know how to protect yourself from an ugly security breach if your in-house computer expert leaves?

What happens if your in-house expert splits with no warning, AND has access to your company's network? As soon as humanly possible, you should disable his or her access, including remote access to your network. As a client of **Hawk iSolutions Group, Inc.**, we can make sure all of the employee's access is disabled the moment you find out that he or she no longer works for you.

So how did you do? If you answered "no" to even one of these questions, you need to get the answers now before it's too late.

Securing Your Wireless Networks

With the increasing deployment of 802.11 (or Wi-Fi) wireless networks in business environments, IT organizations are working to implement security mechanisms that are equivalent to those existing today for wire-based networks.

Three well-known methods to secure access to an AP are built into 802.11 networks. These basic methods are widely available and may be sufficient for some deployments:

- Service set identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

One or more of these methods may be implemented, but all three together provide a more robust solution.

SSID

Network access control can be implemented using an SSID associated with an Access Point or a group of APs. The SSID provides a mechanism to “segment” a wireless network into multiple networks serviced by one or more APs. Each AP is programmed with an SSID corresponding to a specific wireless network. To access this network, client computers must be configured with the correct SSID. A building might be segmented into multiple networks by floor or department. Typically, a client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations.

Because a client computer must present the correct SSID to access the AP, the SSID acts as a simple password and, thus, provides a measure of security.

However, this minimal security is compromised if the AP is configured to “broadcast” its SSID. When this broadcast feature is enabled, any client computer that is not configured with a specific SSID is allowed to receive the SSID and access the AP. In addition, because users typically configure their own client systems with the appropriate SSIDs, they are widely known and easily shared.

MAC Address Filtering

While an AP or group of APs can be identified by an SSID, a client computer can be identified by the unique MAC address of its 802.11 network card. To increase the security of an 802.11 network, each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client’s MAC address is not included in this list, the client is not allowed to associate with the AP. MAC address filtering (along with SSIDs) provides improved security, but is best suited to small networks where the MAC address list can be efficiently managed. Each AP must be manually programmed with a list of MAC addresses, and the list must be kept up-to-date. In practice, the manageable number of MAC address filtered is likely to be less than 255 clients.

WEP-Based Security

Wireless transmissions are easier to intercept than transmissions over wired networks. The 802.11 standard currently specifies the WEP security protocol to provide encrypted communication between the client and the AP. WEP employs the symmetric key encryption algorithm, Ron’s Code 4 Pseudo Random Number Generator (RC4 PRNG).

Under WEP, all clients and APs on a wireless network typically use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. The 802.11 standard does not specify a key-management product, so all WEP keys on a network usually must be managed manually unless they are used in conjunction with a separate key-management. Support for WEP is standard on most current 802.11 cards and APs. WEP specifies the use of a 40-bit encryption key and there are also implementations of 104-bit keys. The encryption key is concatenated with a 24-bit “initialization vector” (IV), resulting in a 64- or 128-bit key. This key is input into pseudo-random number generator. The resulting sequence is used to encrypt the data to be transmitted. (WEP keys can be entered in alphanumeric text or hexadecimal form.)

WEP encryption has been shown to be vulnerable to attack. Because of this, static WEP is only suitable for small, tightly managed networks with low-to-medium security requirements. In these cases, 128-bit WEP should be implemented in conjunction with MAC address filtering and SSID (with the broadcast feature disabled). Customers should change WEP keys on a regular schedule to further minimize risk. For networks with high security requirements, the VPN or emerging 802.11i standards-based solutions are preferable. These solutions are also preferable for large networks, in which the administrative burden of maintaining MAC addresses on each AP makes this approach impractical. The point at which the number of wireless client systems becomes unmanageable varies depending on the organization’s ability to administer the network, the choice of security methods (SSID, WEP, and MAC address filtering), and its tolerance for risk. If MAC address filtering is used on a wireless network, the fixed upper limit is established by the maximum number of MAC addresses that can be programmed into each AP used in an installation. The upper limit varies, but the practical problem of manually entering and maintaining valid MAC addresses in every AP on a network limits the use of MAC address filtering to smaller networks.



Hawk iSolutions Group, Inc.

Hawk iSolutions Group, Inc.
6439 Plymouth, Suite 112
St. Louis, MO 63133

Phone: (314) 727-1174
Fax: (636) 230-9905
www.hawkisg.com

IT Solutions...
helping build
your business

Services We Offer

- PC repair and troubleshooting
- Printer repair and troubleshooting
- Disaster recovery
- System back ups & data protection
- Virus protection & removal
- Network security
- E-mail & Internet setup help
- Wireless networking
- Consulting & support
- One-on-one computer training
- Hardware Sales

ATTENTION SMALL BUSINESSES:

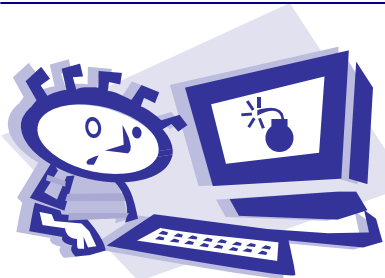
Get all of the computer support you need without the expense of hiring a full time IT staff. Ask about our Small Business Computer Support Program.

Quick Computer Tip:

How To Add A Shortcut To Your Desktop

Do you have a document, folder, or application that you frequently access? If so, you might want to add a shortcut to your desktop to give yourself "one click" access to it without having to navigate the path to the actual location of the file. Here's how:

1. Right-click anywhere on your desktop and a pop-up menu will appear.
2. Select "New," then "Shortcut," and a "Create Shortcut" window will open.
3. Use the "Browse" button to find the path to the application or program.
4. Click on the icon of the program or file that you want, and then click "OK". Click "Next" and then enter a name for the shortcut.
5. Enter the name for your shortcut and click "Finish." The new shortcut will appear on your desktop. Drag the shortcut icon to any place on your desktop.



Beware of "Fun" Web Surveys!

Tell me 10 things about your favorite pet or answer these 20 questions to discover your personality type. You might think this kind of e-mail or web form is a fun way to learn about yourself or communicate with friends, but beware! Spammers and hackers often use these forms to solicit personal information, steal your e-mail address, and spread viruses.

Part of the problem is that people forward these surveys including their friends' e-mail addresses in the text of the email. This allows hackers and spammers to steal your e-mail address and the e-mail addresses of your friends to spread viruses or simply annoy you with endless spam. Best bet: Don't fill out surveys on a web site or an e-mail unless it's with a reputable company for a legitimate reason and never forward them to others.