Importance of Backups and Anti-Virus

Many IT support companies stress the importance of backups in any business. Think about the old saying "Don't keep all your eggs in one basket". This phrase is one of the best when describing anything that is severely important to your day to day operations. Does your business work with customer information like patient history, invoice history, contact information or vendor lists? What about a particular program that you use to create and design your product for your clients? Are you a photographer that works with the cherished memories of your customers? Every business from an accountant to an x-ray technician has some type of important data that is needed for their business to function. But what happens if that data was to disappear one day? Disasters happen. Equipment failure, natural disasters, theft, malicious intent and viruses are some ways your data can become lost. What happens then?

With a proper managed service provider, you should not have to worry about this. Most managed service providers have plans that include local and offsite backups. There should always be a 3-2-1 approach to your backups, 3 copies of any important data (1 primary and 2 backups). There should always be 2 different types of media being used like hard drives and optical drives to protect against different types of disasters. One copy should always be stored offsite (such as a cloud backup) in case there is a disaster in the general area of your business.

Some of the threats to your data out there are not so easy to spot. Here we will review some of the major culprits that can destroy your data.

Viruses

Viruses are created daily at an alarming rate with totals reaching over 300,000 a day. Because of this, anti-virus programs do their best to identify and neutralize many of these threats before an outbreak occurs. One of the nastiest viruses to date has the ability to completely encrypt your network's data and hold it for ransom for costs upwards into the thousands of dollars. All operating systems are susceptible to virus attacks (yes, even Macintosh computers) and because of this, your data can be compromised. The best protection against these types of viruses (aside from a strong anti-virus package) is a cloud backup that offers the ability to restore a file from a previously uploaded version. Another option is using media that is considered "write once storage" like a CD/DVD since the data cannot be manipulated directly on the device.

Malicious Intent

Any computer with internet access is theoretically susceptible to a "hack attack". This would be a hacker compromising your network and accessing your database of sensitive files. With this level of access they can do anything from copy it and sell it on the black market to destroy it for "the fun of it". To prevent this, always have strong passwords for any logins and install a business grade security firewall on your network.

But what about a computer that is not on the network or online? Even then you are not protected from malicious intent if anyone has access to your data (such as your invoicing computer). All it takes is a disgruntled employee to access the info or the computer itself, destroy the machine (either physically or with the use of software tools) and that's it. POOF! Your data is gone. Any type of physical backup is recommend for this such as a set of external hard drives that are rotated daily locked in a safe nightly. Some businesses may also benefit from one of the backups being taken home with the owner each day

to ensure an offsite copy is available. This does require extra work but if it is for the sake of your business, isn't it worth it?

Theft

Theft is a common concern for any business. But what about when the thief is not stealing your goods but rather, your client information? A thief may be out to break into a business to steal equipment like laptops, desktops, cameras, etc…. They may be looking to steal this just to sell it to a pawn shop for some quick cash. The issue is that the computer that they may have stolen is the one that has your business files stored on it. They may not have intended to steal this, but what happens if you don't catch the culprit? Without a proper backup, you may never get those files back. This is where a cloud based backup is the best as it is stored offsite with no physical items available to be stolen.

Natural Disasters

Natural disasters are something that we have no control over, we can only prepare in case one occurs. However, it does not have to be a disaster to still affect your data. Some common weather occurrences can affect your equipment, and in turn your data. Some people may think of a fire or a flood which are somewhat common, but there is something that is even more common to us that is usually overlooked. Think of a thunderstorm. Not many people would classify this as a natural disaster but it can wreak havoc on your business. Many business can be destroyed by a lightning strike that causes a surge throughout the office. Equipment becomes surged and rendered useless. Computers are especially sensitive to electricity. If there is excessive voltage or rapid loss of power, data can become corrupted. This is where optical and offsite backups are best.

Equipment Failure

It is not a matter of "if" but "when" will a piece of equipment fail. Anything that is built breaks down over time. Sometimes, it may fail 6 months after purchase or it may last you 10 years longer than expected. However, it is a matter of time before it will no longer operate the way it should. If you do not have a good backup of you main system, how long will it take you to get back up and running like normal? The best preventive way of protecting against this is to have a system image backup. This is where your computer is cloned and backed up to an imaged state. This way, it can be restored to a different PC in a matter of hours to the point that it was last backed up at. Regular image backups are an essential way to keep your data intact and readily available if equipment failure should occur.

After reviewing all of these possibilities, ask yourself: Am I ready if a data disaster affects me? If you have any questions about this, you should seek the advice of an IT consultant.

Anti-Virus

Earlier we touched upon how viruses can affect your data. But that is not the only thing that viruses do. They can target one computer in a variety of ways. Maybe an employee opened an email attachment that contained a virus or they were on a website they should not have been visiting while at work and contracted a "fake" anti-virus popup? It does not take much to encounter a virus since hundreds of thousands of them are created daily. But what happens if you do stumble across one? This is where a strong anti-virus package comes into play.

Many managed service providers offer anti-virus plans. We find that there is no anti-virus that is 100% effective against all viruses. The best steps are actually a multi-pronged approach to virus protection. This includes using an AUP with your employees so they understand the dangers of using the business equipment for their personal use, an alternate web browser that is not included with your operating system (like Google Chrome and Firefox), an ad-blocking add-on to your browser and not only an anti-virus but a malware protection program as well. If you are not sure if you have the correct protection, ask your current service provider. If you do not have one yet and are still in the search for one, ask about the details around their anti-virus protection plan.

Redundancy and Support

Redundancy is something you should always plan for, whether it is a backup of your data or your hardware itself. Nowadays, servers have the ability to have redundant hardware in them. This can be from power supplies, hard drives, network cards and processors. What happens is if one part fails, the redundant part takes over without the need for a restart or shut down of the system. It allows for the time to get a replacement part onsite and into the machine without all the downtime associated with hardware failure. These parts can sometimes be “hot-swappable” meaning that you can take out the failed part and replace it with a new one while the machine is still running. Another side to this is when hard drives come into play. A RAID allows one main hard drive to be in use while a second, backup drive is constantly coping the data to itself. If the main drive goes down, the other kicks in and continues to work. An alert is then sent to your managed service provider letting them know that there is an issue and they are able to address the issue quickly before you even knew there was a problem.

What happens if there is an issue and you need immediate assistance? How long can you wait before your business is dramatically affected by the downtime? Many businesses have standard operating hours (say 8am to 5pm). But what about yours? Are you a retailer open until 11pm daily? What about a machine shop that runs with a third shift crew? What do you do when emergencies happen?

Most managed service providers operate during standard hours during the day. They are on call and available during their normal business hours in which case, you could call them with an issue and they will respond in their standard time window. However, how far are they from your location? If you outsource your IT, you may end up waiting a while depending on their standard ticket response time. For most businesses, that is a 4 to 6 hour window before someone will even acknowledge you have a problem. Can you wait that long for service? After the ticket is acknowledged, it will be assigned to a tech and they will start a remote session, a common practice among IT support where you allow your service provider access to your computer via the internet. They can control your PC as if they were sitting in front of it. Conversely, what if the issue you have cannot be fixed through remote service? What if the computer does not turn on or does not connect to the internet? If they are not a local company, they may not even provide onsite service for emergencies. What do you do when they? When a vital system goes down, will you be ready?

Look for a managed service provider that is local, offers onsite, remote and in-house support. Another great feature to look for is if they provide emergency contact numbers in case something happens outside their standard business hours. Check to see who gets those emergency calls as well. Do they just go to an answering service or to they go to the people that directly work with your business. You would

be surprised to find out how many offer after hours service that is outsourced overseas and is remote support only. Do not fall into that trap!

Now that we have gone over some of the ways your data can become compromised and the best steps to take to protect your data and your business, ask yourself: Does my managed service provider provide all these services? Most do, but at an extra fee. SNECS includes a multi-pronged anti-virus package, 24/7 emergency contact numbers as well as local and offsite backups included with their Office Solutions plans.