4 REASONS WHY BUSINESSES NEED TO REGULARLY BACK UP INFORMATION

It doesn't matter how big your business is, regular backups are essential to securing your company's data. In fact, regular backups may arguably be the single most important step you take for preventing a disaster.

Backups help ensure that regardless of your current security strategy, you have secure and clean data to keep your business running in the case of data loss, a hack attack or even a natural disaster.

HERE ARE FOUR REASONS YOU NEED TO IMPLEMENT A PROPER BACKUP STRATEGY.

1 FAILURE TO REGULARLY BACK UP INFORMATION COULD COST YOU SERIOUS MONEY

Regular backups are an insurance policy for your business. With so much of the modern business supported by computer networks, a loss of your network data can have a crippling financial effect on your business.

A major survey of IT leaders from over 24 countries reported by Security Week found that incidents which led to data loss have increased by 400 percent in the last two years, for a combined loss of $1.7 trillion due to network downtime and data loss.

2 RANSOMWARE CAN STRIKE AT ANY TIME

Another trend that is growing across the world is the spread of ransomware. Once you're hit with ransomware malware, your entire network is encrypted. At that point you're locked out of your own network until you pay a ransom to hackers, usually with a crypto-currency like Bitcoin.

Don't assume that your small business might fall under the radar from this type of attack. Due to their lack of security, small businesses are often the prime targets for ransomware attackers. With a secure backup of your system, you can help avoid paying the ransom and simply restore your data before you were infected with ransomware.

3 WITHOUT BACKUPS, NATURAL DISASTERS COULD PUT YOU OUT OF BUSINESS

Statistics indicate that 40 percent of businesses fail to open after suffering a natural disaster and additional 25 percent fail within a year. Part of the problem has to do with failure to backup data, leaving businesses starting from scratch following a disaster.

Unfortunately, many businesses still don't perform proper backups. For example, one study found that 60 percent of small businesses don't back up daily and many don't perform backups at all.

4 REGULARLY BACKUP INFORMATION PROVIDE PEACE OF MIND

Backups help you rebuild your network regardless what happens. Otherwise, you can lose important data like customer financial records, product information, payroll data, mailing lists and business plans. If a virus starts destroying your network, failure to restore your system from a clean backup can leave you with network outages that can last days or longer, destroying customer confidence in the process.

In some cases, it's not a matter of hack attacks or malware, but simple data corruption. Backups help you go back in time before you experienced network issues and quickly restore your network. It's no exaggeration to say that even one incident of major data loss can mean game over for your business. Backups ultimately allow you to focus your business efforts on what delivers value instead of always looking over your shoulder for a network security disaster.

THE RIGHT BACKUP STRATEGY

Cloud Backups: Cloud backups are an essential part of a smart backup strategy. Cloud backups help ensure that if your business suffers a natural disaster, you are able to restore your data off-site.

Encryption of Data In-Transit: Backup data should be encrypted when in transit, otherwise hackers can snoop on data. A smart encryption plan is key to overall data protection across your network.

One of the timeless rules that can effectively address any failure scenario is called the 3-2-1 backup rule. This approach helps to answer two important questions: how many backup files should I have and where should I store them?

The 3-2-1 rule became a popular concept thanks to Peter Krogh, a well-known photographer who wrote that there are two groups of people: those who have already had a storage failure and those who will have one in the future. In other words, the 3-2-1 backup rule means you should:

- Have at least three copies of your data.
- Store the copies on two different media.
- Keep one backup copy offsite.

Davichi