Data security

This is critical for most businesses and even home computer users. Client information, payment information, personal files, bank account details - all of this information can be hard to replace and potentially dangerous if it falls into the wrong hands. Data lost due to disasters such as a flood or fire is crushing, but losing it to hackers or a malware infection can have much greater consequences.

Risk Assessment

Thorough data security begins with an overall strategy and risk assessment. This will enable you to identify the risks you are faced with and what could happen if valuable data is lost through theft, malware infection or a system crash. Other potential threats you want to identify include the following:

· Physical threats such as a fire, power outage, theft or malicious damage

· Human error such as the mistaken processing of information, unintended disposal of data or input errors

· Exploits from corporate espionage and other malicious activity

You can then identify areas of vulnerability and develop strategies for securing your data and information systems. Here are several aspects that need to be considered:

· Just who has access to what data

· Who uses the internet, email systems and how they access it

· Who will be allowed access and who will be restricted

After the above analysis, you can then prioritize specific data along with your more critical systems and determine those that require additional security measures. It is also a good idea to layout a BCP (Business Continuity Plan) so that your staff is still able to work effectively if the systems happen to fail. Company risks and security implementations should be reviewed frequently to support changes such as the growth of your business and other circumstances.

Securing Data

Once you draw up a plan and assess your risks, it is time to put your data security system into action. Since data can be compromised in many ways, the best security against misuse or theft involves a combination of technical measures, physical security and a well educated staff. You should implement clearly defined polices into your infrastructure and effectively present them to the staff. Here are things that you may do:

· Protect your office or data center with alarms and monitoring systems

· Keep computers and associated components out of public view

· Enforce restrictions on internet access

· Ensure that your anti-malware solution is up to date

· Ensure that your operating system is up to date

· Fight off hacking attacks with intrusion detection technology

· Utilize a protected power supply and backup energy source

Mobile Data Security

Hand-held devices and laptop computers have become popular in the business environment. However, mobile computers are at a much greater risk of data loss through damage and theft. For this reason, different safeguards need to implement in addition to the security measures listed above.

· Regularly backup data on removable media and safely store multiple copies

· Activate password protection whenever the device is left alone

· Never leave the device alone and visible in a vehicle

· Protect the device from physical damage by transporting it in protective casing

Efficient data security involves numerous steps, many of which can be downright time consuming. On the other hand, I am sure you will agree that actually losing this important data could be much worse.