Bulletin No. CP 10
File: Corporate Planning

Bulletin

Things and Must Do's to Protect/Secure Your Company's Data

INTRODUCTION

In today's technologically driven world, businesses of all sizes are producing enormous amounts of data and information, and much of it is in electronic form. Operating policies and procedures, history files, personnel files, financial information, customer data and much more are stored in computers and related computing equipment. And, computing skills are needed to find business operating information.

Data stored in a computer should be more secure right? Maybe not. One major flaw in many small and medium size business plans is not having a data disaster backup and recovery plan. Disaster can come in many different forms. Natural disasters such as floods, fire, tornados and hurricanes can wreak havoc on business data. But so can theft, computer hacking, computer viruses or disgruntled employees.

According to the U.S. Small Business Administration, 25% of businesses never reopen after being hit by a disaster. A data storage and backup strategy is essential to business continuity.

Fortunately, today, data storage technology is cost-effective and readily available. Data storage comes in all shapes and sizes and is very customizable to accommodate varying business storage requirements.

DATA STORAGE SOLUTIONS

In general terms, Data Storage Solutions fall into several different categories:

1. **Direct Attached Storage (DAS)**
   DAS refers to storage devices that are directly connected to a personal computer (PC) or a server. This is generally the weakest of all data backup plans. The system requires periodic one-off or batch type backups, which may result in old and outdated data. In addition, the storage device is in the same location as the data itself, a potential security issue.

2. **Network Attached Storage (NAS)**
   NAS are storage devices directly connected to a network. This strategy utilizes a file server or virtual server which can accept multiple storage devices and has the ability to automatically synchronize data.

3. **Disaster Protected Storage**
   This strategy uses on-site or off-site fire-proof and water-proof storage safes to house data discs, drives and related storage devices. This solution allows a user to bring home a tape backup of the periodic data every night or have the backup media couriered to an off-site location periodically.

4. **Online Storage**
   Often referred to as Cloud-Based solutions, online storage offers the best option to secure data, especially for businesses that do not have their own on-site server equipment. Cloud storage can back up data incrementally and periodically throughout the day and does not require any significant capital investment. Storing your data at an off-site location is an easy way to ensure that a copy of your data is protected from most types of disaster.

DATA SECURITY SOLUTIONS

Redundancy of data backup is important. Do not rely on just one data source. However you choose to store your data, make sure at least two full copies are maintained on separate devices in separate locations. Overriding factors to data storage involve the volume of data you are seeking to protect and your available budget to do so.

Listed below are a few tips on safeguarding your business data:

1. Consider local storage of your frequently accessed data either in secured folders on a server or in encrypted databases.

2. Set permissions in both cases so files can only be accessed by authorized personnel. Others trying to access the data will be denied.

3. If your servers are located at your business, consider storing them in a locked server room to which only authorized personnel can enter.

4. For business networks, make certain that all network user accounts are password-protected. Complex passwords should, as a policy, be changed frequently. Employees should not be allowed to share their passwords with other users. They must either log off or lock their sessions if they leave their work areas.

5. Each enterprise software application should require unique login authentication. Users are provided access as required by their position with approval from senior management.

6. Should your business require any type of remote access, it should be accomplished through a multi-layer security device requiring authentication that uses encrypted sessions.

7. If some of your data enters your system from outside locations, remote access can be accomplished using either VPN or RDS (Remote Desktop Server). Both require users to authenticate with a username and password.

8. Consider giving data access on a “need to know basis” and extend that condition to the rest of the user base. Enterprises should adhere to the “least privilege” model of resource access.

9. Special attention should be given to email. Email is a primary attack vector for hackers!

a. Communication should be protected through several different layers of filters. For example:

   i. Internal third party packages
   ii. External third party services
   iii. Rules and policies established within the mail server

10. Virus protection and software patching should be installed on all machines and servers and updated in a timely manner.

11. In-line backup with replication is preferred for all servers. Autonomous cloud backup can be provided for individual user's data protection.

12. Administrative access should be severely restricted to a few users.

13. Consider an Intrusion Prevention System to stop external hacks to your network.

DATA PROTECTION STRATEGY AND POLICY

Every business should develop and implement a Data Protection Strategy and Policy. The policy should outline proper use of business data and communication systems to safeguard against unwanted access by third parties. Although such a policy is generally based on common sense, it should be provided to all employees in a written document so that they do not unknowingly allow your company's information to fall into the wrong hands.

Some general guidelines to an effective data systems strategy are outlined below:

- Establish email and Internet security policies and standards.
- Monitor compliance with security requirements.
- Prepare a computer emergency strategy to respond to virus infestations and hacks.
- Periodically conduct a risk assessment of each production information system.
- Maintain strong user access controls consistent with the need-to-know level of information.
- Assure proper and secure deletion of sensitive information when it is no longer needed.
- Do not allow unauthorized individuals to access your business network.
- Do not allow connection of any unauthorized device to your business network.
- Minimize the use of business resources or Internet connectivity for any purpose other than business use.
- Maintain exclusive control over logins and passwords and protect them from inadvertent disclosure to others.
- Employees should immediately report to appropriate company IT staff any loss of data or equipment, malicious software or erratic system behavior.
- Always log off business systems at the end of the day.
- If sensitive information must be sent externally by electronic means, consider encryption or similar technology to protect the data.
- All information taken from the Internet should be considered suspect until confirmed by a separate source. There is no quality control process on the Internet resulting in an increased level of risk.

CONCLUSION

In the end, there are a variety of available options to secure your company's data. Technology is changing every day. The key elements of protecting your business data are:

1. Develop a disaster recovery plan.

2. Evaluate the options that fit the capacity of your business data volume and find a suitable data storage solution.

3. Consider your IT budget.

4. Don't wait for a disaster to happen before you implement a strategy.

References

Business News Daily
"22 Cloud Storage Solutions for Small Business," Sara Angeles, Staff Writer, October 17, 2017

CIO
"How to Build a Storage and Backup Strategy for Your Small Business," Paul Mah, Fellow, March 11, 2014

PC World
"4 Ways to Disaster-Proof Your Data Backups," Paul Mah, October 1, 2013

