PREPARED
SMALL
BUSINESS

Top Ten Things Small Businesses Must Know About Protecting and Securing Their Business Data

By Donna R. Childs

Most small business people would likely agree that securing and backing up their data are critical to their businesses. But many of these businesses are not employing the best practices for data security and backup. The following are the top ten things small businesses must know about securing and protecting their business data presented in order from most common to least common practices of small businesses. How many of these practices are you following in your business?

1 ***Small businesses must know which data they need to secure and protect.***

Is it customer information, human resources information, proprietary trade secrets, financial and business information? You must be able to prioritize your information needs to determine what is critical to secure and protect for your business. Data that are critical must be secured against a variety of threats from malware to viruses to phishing schemes. These critical data must also be backed up for ease of retrieval in the event that the primary information files are lost or damaged.

2 ***Small businesses must have procedures in place for digitizing and storing important information that cannot be retained exclusively in paper format.***

This would include critical documents such as offices leases or signed tax returns, for example. These documents should be scanned and retained electronically. As they contain sensitive information, they must also be protected against security threats.

3 ***Small businesses must give some thought to the lifecycle of information management.***

You need to determine which information must be protected and for what period of time. It is not productive for any small business to secure and back up information that has become obsolete. This will require some discipline for properly disposing of out-of-date electronic files.

4 ***Small businesses must ensure that business data that are no longer needed are securely purged.***

Failure to properly delete business data from your hardware including mobile devices puts your business at risk, both for security breaches and for operational errors, such as backing up information that is out-of-date.

5 ***Small businesses need to understand their regulatory and compliance requirements for securing and protecting business data.***

A physician's medical practice, for example, has specific legally mandated requirements for the protection of patient data. All small businesses have specific requirements for the length of time by which tax and payroll information must be preserved.

6 ***Small businesses need to establish file-naming conventions to ensure that secured, protected business data are properly identified.***

According to the Butler Group , businesses spend 10% of their payroll searching for files and information. This is an expense small businesses cannot justify.

7 ***Small businesses need to ensure that all staff know the proper procedures for protecting business information***

Business security is only as good as its weakest link. Small businesses must also ensure that staff know how to retrieve information from backups if necessary, as skilled IT staff may not always be available to lead a data recovery operation.

8 ***Small businesses should have automated processes for protecting and backing up data.***

Approximately half of all small businesses that back up data do so manually, which puts them at risk for disruption. Automating the backup process ensures that it is not forgotten or overlooked when demands on staff time intensify.

9 ***Small businesses must protect their data with secure off-site backup facilities.***

Many small businesses back up their data onsite, which means that in the event of a disruption, such as a fire or flood, they will simultaneously lose access to both their primary data and the backup.

10 ***Small businesses should test their backups to ensure that they are protecting the information that they think that they are protecting.***

The beginning of the data recovery process is the worst time to learn that certain of the files critical to the business were not stored as planned.

According to a survey of the National Federation of Independent Businesses, the typical small business will experience a disruptive event lasting more than 24 hours on average, once every three years. These events can be computer viruses damaging networks or servers or floods requiring the evacuation of the office; relatively trivial events that commonly occur. So protect your small business against the certainties of disruption by putting in place good practices for protecting business data. It will give you peace of mind and help your business to operate more efficiently.

Donna R. Childs is the author of Prepare for the Worst, *Plan for the Best: Disaster Preparedness and Recovery for Small Businesses* (Second edition, John Wiley & Sons Inc., 2008). She is the owner of a small business with projects in Asia, Africa and Europe. Her website is www.preparedsmallbusiness.com.