Small Business Data Protection

What Small Businesses Need to Know

Authored by

SMB Group
Actionable Market Insight

Sponsored by

DELL EMC

Contents

Introduction 3

Why You Can't Afford to Be Complacent About Data Protection and Security 4

Data Security vs. Data Protection: What's the Difference? 5

Data Backup and File Sync and Share: Why You Need Both 6

Data Backup: What to Look For 7

File Sync and Share: What to Look For 8

Comparing Data Protection Solutions 9

Recommendations for Small Businesses 10

About 11

Sources 11

Introduction

The way we work is changing. Technology has become part of the business fabric, and our ability to effectively harness data is critical to business survival and growth. We expect to have the information we need available when and how we need it—to collaborate, transact and make decisions.

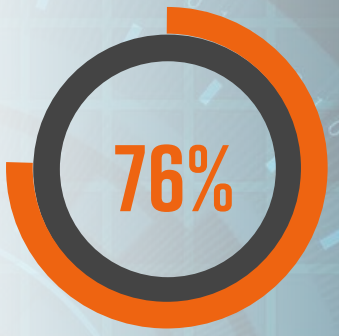
But as our reliance on technology grows, so do the requirements to access, secure and protect data. In fact, small businesses rank “keeping systems up and running” and “securing/protecting my company information from threats” as their most pressing technology challenges.

System downtime obstructs access to the data and files you need to get work done—and can result in serious consequences. Productivity suffers, revenue drops and businesses struggle to recover. Security breaches—from ransomware to hijackings, and phishing to worms—can result in severe financial and brand damage.

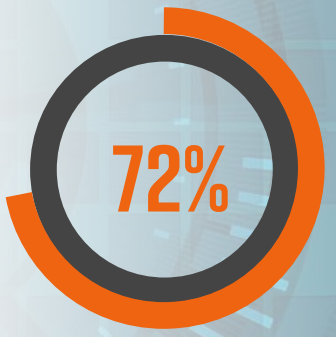
But for most small businesses, technology expertise is a scarce resource. As a result, many of these companies put security and data protection on the back burner—a risky bet as more data is distributed across more places and devices.

In this ebook, we discuss how your small business can address these issues in a practical, effective way. We start by discussing the importance of safeguarding your business in the digital age, as well as the difference between data security and data protection. Then we take a deeper dive into data protection and file sync and share solutions, and we offer recommendations about what you should look for in these solutions. In our companion ebook, **Small Business Data Security**, we focus on what you need to know about security for your small business.

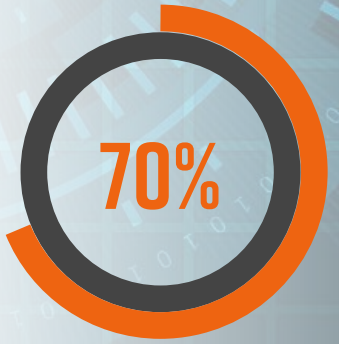
The Impact of Technology on Small Businesses[1]



Agree/strongly agree that digital technology is reshaping our industry



Agree/strongly agree that using new technology effectively is key to our company’s survival and growth



Agree/strongly agree that digital technology is reshaping our company’s business model

Why You Can't Afford to Be Complacent About Data Protection and Security

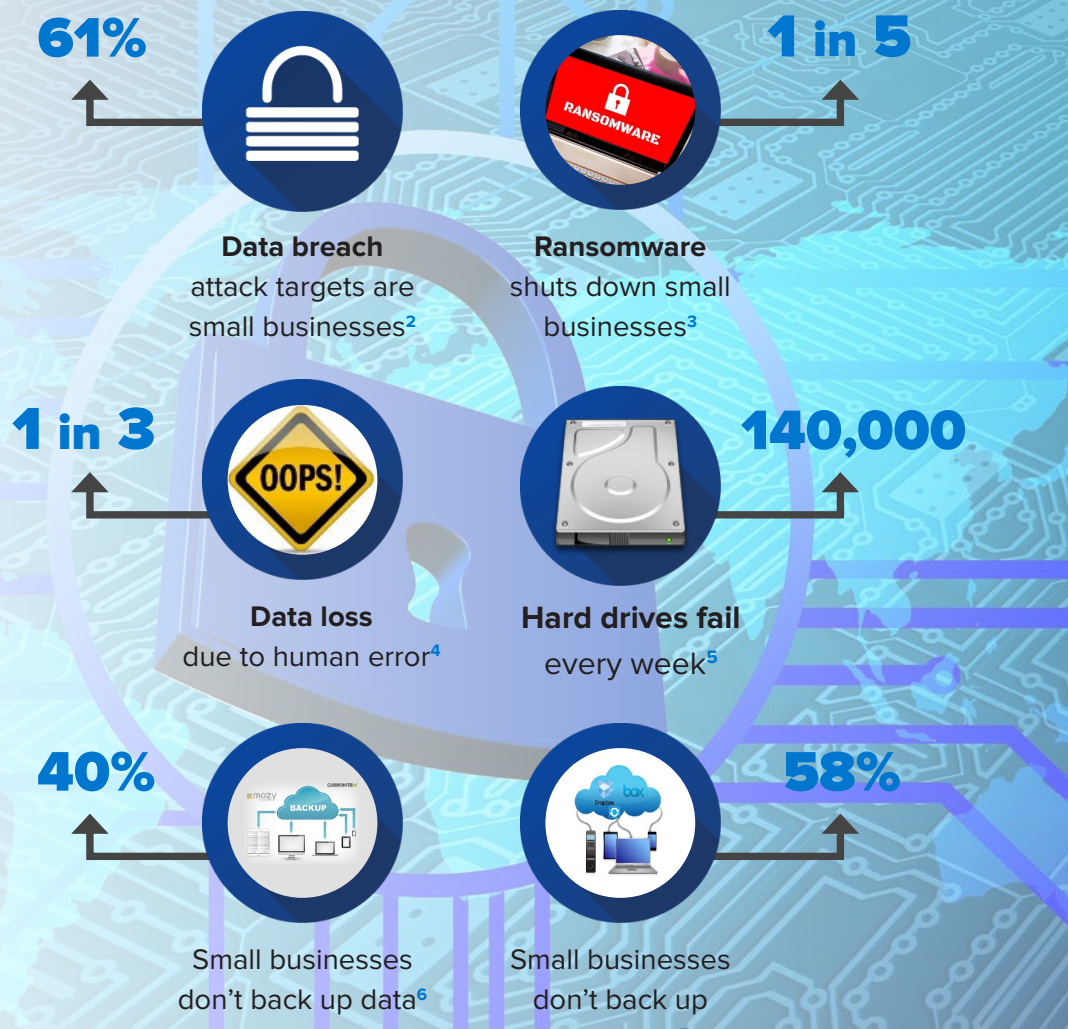
Some small business decision makers think that because their companies are small, they don't need to worry about cyber attacks and data breaches. For example, 40% of small businesses don't back up any of their data, and 58% neglect to back up client devices (aka "endpoints"). Especially in today's always-on, mobile world, this is an increasingly risky strategy.

Small businesses are more vulnerable than ever to security threats and data loss. Consider the following statistics:

- **61% of data breaches hit smaller businesses in 2016, up from 53% in 2015[1].**
- **1 in 5 small businesses were the target of a ransomware attack and experienced a shutdown due to the attack[2].**
- **1 in 3 small businesses experienced a data loss due to human error[3].**
- **140,000 hard drives fail every week in the United States[4].**
- **1 in 4 mobile apps include at least one high-risk security flaw[9].**

Data-related outages and downtime can carry heavy costs—leading to reputation damage, loss of customer trust and financial damage resulting from the inability to get the information you need to get work done, and from potential fines and penalties. In the worst-case scenario, a small business may not even recover if the infected data or system cannot be restored expeditiously. But you can avoid these issues by taking a few proactive measures to guard against data loss and security breaches.

93% *According to the Online Trust Alliance's analysis of security breaches reported through 2017, 93% of data loss incidents were avoidable.*



Data Security vs. Data Protection: What's the Difference?

The first step to protecting your business in the digital age is to understand the distinctions between data security and data protection. Both are critical to protecting business-critical data—but they have very different roles and help defend against different types of vulnerabilities.

Data security solutions

help prevent unauthorized access, use, disruption, modification or destruction of data stored on servers (either on premises or in the cloud) or client endpoint devices, including both traditional desktops and mobile devices. They are designed to keep company data safe from any kind of nefarious exploitation, including both internal and external threats. Data security solutions prevent malware attacks and also prevent hackers from gaining access to systems.

Data security solutions include the following:

Cyber security solutions

Identity and access management (IAM) solutions

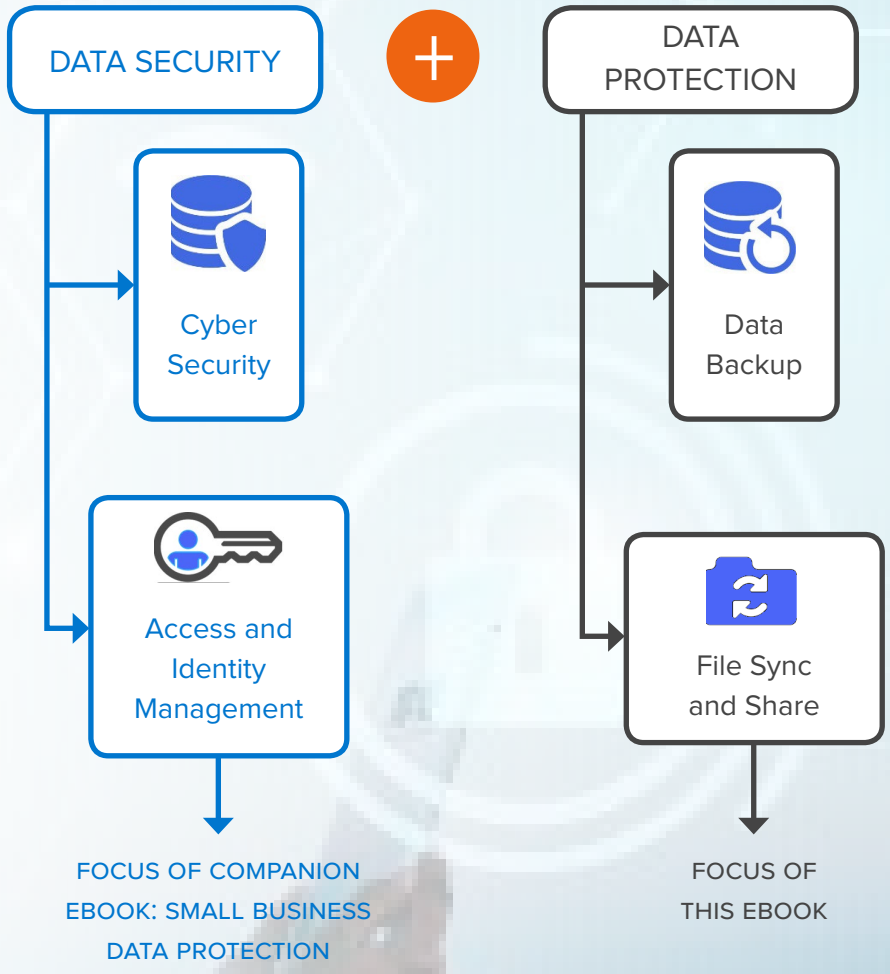
Data protection solutions

provide a mix of services to protect companies from data loss and downtime. These solutions restore data that is compromised at the system level or the file level, whether as a result of data security attacks, device loss, employee negligence or natural disasters, such as hurricanes and floods.

Data protection offerings include the following:

Data backup solutions (on premises, cloud and mobile)

File sync and share solutions



Data Backup and File Sync and Share: Why You Need Both

Both data backup and file sync and share (FSS) solutions can help you protect your business data, but each has different advantages and serves different objectives.

Data backup solutions enable users to recover and restore data in the event of data loss, whether due to malfeasance, errors, a lost device or a natural disaster.

Data backup business benefits include the following:

- Restoration of data if it is impacted or accidently deleted, or if a device is lost
- Safeguarding against system and/or hard drive failure
- Availability of data over time to support regulatory compliance

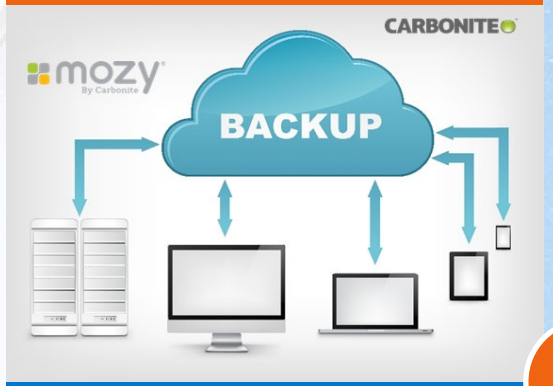
File sync and share solutions give users easier access to the data they need and enable them to share that data on any device they use. These solutions also enable the sharing of that data among teams of internal employees and external collaborators.

File sync and share business benefits include the following:

- Quick access to files by multiple devices or employees
- Reduced need to store multiple copies of the same data on multiple devices
- No need to email files
- Access provided to a copy of a file if it is corrupted or deleted
- Integration with business and productivity applications, which improves user productivity and experience

Data Protection

Data Backup



- Provides data replication, data recovery, data archiving
- Restores data if it is lost due to unauthorized users, malware, device loss, natural disasters, etc.
- Provides online access to data during recovery process

File Sync and Share

- Stores documents in a centralized, cloud-based location
- Enables authorized users to easily access and share files
- Provides document management and version control
- Facilitates collaboration between both internal and external users

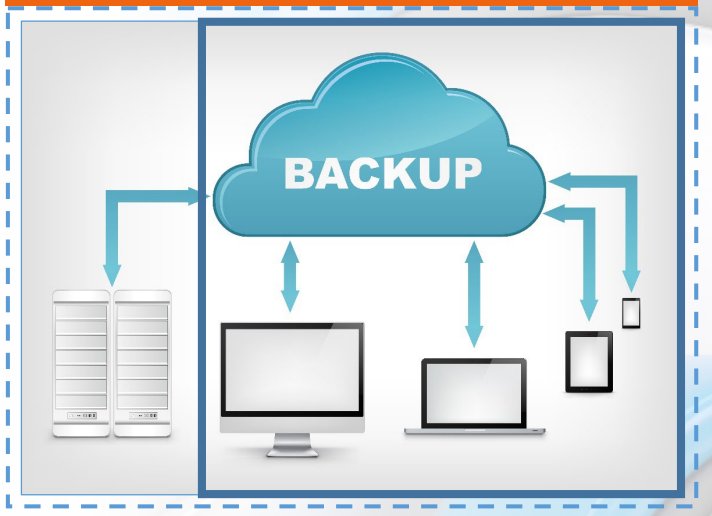
Data Backup: What to Look For

Complete system data backup should include the following features:

- Backup of all infrastructure: servers, endpoints, storage systems and cloud data
- Storage of a backup copy in the cloud via a cloud service provider and a secure subscription service
- Data encryption for data sent to the cloud backup service provider data center
- Incremental backups (as data changes) after initial backup
- Detection and backup of new/changed files to minimize the impact on performance and user productivity
- Data de-duplication support to improve performance and reduce storage and bandwidth requirements
- Use of backups captured as a point-in-time snapshot to restore data to its previous state from any previous point in time
- Recovery capabilities at a system, file or bare-metal level
- Pricing tiers based on cloud storage capacity and/or the number of devices included in the backup

Companies that offer small business– focused backup solutions include Mozy and Carbonite.

Data Backup



Endpoint backup (laptop, PC, mobile devices)

Complete system backup (endpoint + servers + storage + cloud)

Endpoint backup should include the following features (special instance of system backup):

- Creates a secondary copy of data stored on user endpoint devices, making data on these devices recoverable if the device and/or data on it are lost or compromised
- Includes all the functionality in the complete system data backup solution
- Easily restores files via the client app

Companies that offer small business–focused backup solutions include Mozy and Carbonite.

Small Business Data Backup Coverage

Protected Infrastructure

- Endpoints: desktops, laptops, tablets, smartphones
- Cloud applications
- Virtual servers
- Servers
- Storage systems

Data Types

- Folders and files
- Email
- Database
- Application data
- Operating system
- System settings

Data Protection Services

- Backup and recovery for the following incidents:
  - Human error
  - Lost devices
  - Overwritten files
  - Malware and ransomware attacks
- Business continuity and disaster recovery
- Archival for long-term compliance support

File Sync and Share: What to Look For

FSS Capabilities

- FSS solutions provide access to files via any internet-connected device from any location without the need for a corporate VPN or firewall.
- Users have the ability to select the files they want to sync and share, which are then placed in a single, special directory on the desktop created by the FSS application.
- File encryption is provided both “at rest” and at the FSS provider cloud data center.
- Users have the ability to share files with other users, both inside and outside the organization.
- FSS solutions provide integration with directory services, such as Microsoft Active Directory, for authentication and access control, and with business apps for easy and direct access to files.

FSS Security Shortcomings

- FSS solutions primarily replicate data on endpoint devices and not the complete IT infrastructure.
- Business-class FSS products offer some security features (such as support for directory integration and single sign-on)—but they are NOT security solutions.
- When malware infects a user’s endpoint files, it will spread through local files and compromise them. And when synced, the infected files will spread to the FSS cloud storage copy.

Small Business File Sync and Share Coverage

Supported Infrastructure

- Endpoints: desktops, laptops, tablets, smartphones

Data Types

- Folders
- Files

Data Protection Services

- File sync
- Sharing files with people inside company and outside for collaboration
- Sharing links to files instead of sending files through email
- Accessing files directly from business applications such as Salesforce.com and Oracle NetSuite

Comparing Data Protection Solutions

	Cloud-Based File Sync and Share Solutions		Cloud-Based Backup Solutions	
Pros	These solutions are used for the following reasons: • They are convenient and easy to use. • They store files in a centralized cloud location. • They sync files across devices. • They share files among various devices and with coworkers.		These solutions are used for the following reasons: • After initial setup, backup works in the background based on set policies. • They do not rely on a single folder to sync data. • They allow manual drag-and-drop of files to the sync folder. • Point-in-time copies of files are stored and can be recovered. • Files are encrypted before moving to the cloud through a secure tunnel. • They enable recovery of data/files following human errors, security breaches and natural disasters. • They provide better support for compliance and legal investigations.	
Cons	These solutions have the following drawbacks: • Potential loss of data through accidental deletion or overwriting • No replication of files or folders that are not included in the sync folder • No deep versioning of files and no long-term retention of data • Potential syncing and sharing of files impacted by malware, resulting in the further spread of corrupted files • Lack of support for business continuity and disaster recovery (BCDR)		These solutions have the following drawbacks: • Limited support for file-based data sharing • Potential for difficulties in the restoration process if the solution is not tested regularly	
Apps	• Dropbox: Dropbox Business • Box	• Citrix: ShareFile • Hightail	• Carbonite: MozyPro for Business • Carbonite: Carbonite Cloud Backup	• IDrive: IDrive Small Business • Acronis: Acronis Backup

Recommendations for Small Businesses

If you haven't already done so, now is the time to work with your service provider to conduct a thorough self-assessment of your existing data protection policies and processes to identify gaps and determine how to fill them.

As you move ahead to safeguard your business better, consider the following steps:

1. **Take a proactive approach.** Don't wait for employees to start using consumer tools. If companies don't provide these tools, employees will adopt them through their personal accounts, creating a more significant management and control issue.
2. **Create a data protection policy with your service provider.** It should contain best practices that employees are expected to follow.
3. **Train employees in security policies.** Establish basic security practices and strategies for employees, such as requiring strong passwords, and develop appropriate internet use guidelines that detail penalties for violating company cyber security policies. Establish rules on customer privacy and the protection of customer information and company data.
4. **Create a mobile device action plan.** Mobile devices (specifically "bring your own device" [BYOD]) create significant data protection challenges. This step is becoming increasingly important in light of increasing regulations and privacy concerns.

5. **Regularly back up the data on all computers and endpoints.** Ensure the backup solution under consideration is available in the cloud as a secure subscription service. Automatically back up the information stored on servers and endpoints.
6. **Regularly test the backup and restore functions.**

7. **Subscribe to file sync and share.** Develop policies and select a business-grade FSS provider early on—otherwise, employees will adopt consumer versions.
8. **Develop policies** for consistent file-naming conventions, versioning and retention. This will make the file sharing function a lot easier.

Read our companion ebook, **Small Business Data Security**, for more information on what you need to know about security.

About

DELL EMC

Dell Small Business Central

Dell has over 30 years of experience partnering with small businesses to help them thrive. We're using that experience to help you guide your small business' success today and far into the future.

SMB Group
Actionable Market Insight

SMB Group is a research, analysis and consulting firm focused on technology adoption and trends in the small and medium business (SMB) market. Founded in 2009, SMB Group helps clients to understand and segment the SMB market, identify and act on trends and opportunities, develop more compelling messaging, and more effectively serve SMB customers.

Sources

1. SMB Group 2017 Routes to Market Study
2. Online Trust Alliance Cyber 2017 Data Breach Investigations Report
3. CNET, "Ransomware shuts down 1 in 5 small businesses after it hits" (assessment of cyber security company Malwarebytes)
4. Online Trust Alliance 2017 Cyber Incident & Breach Trends Report
5. Seagate, "Tips for What to Do If Your Hard Drive Fails"
6. IDGresearch.com, 2015
7. IDC Study, 2015
8. Spiceworks 2018 State of IT Report
9. NowSecure 2016 Mobile Security Report