CRASHPLAN
For Small Business

The Perfect Guide to Backup

5 Keys to Build a Better Backup Strategy for Imperfect Humans

The biggest data loss risk is right in front of you

Read today's headlines, and you're likely to find yet another well-known business victimized by cyberattack. It's not just the big-name brands anymore, either. Two in three data security incidents hit smaller businesses last year, and that number keeps increasing.[1]

The upshot of the constant cyberattack headlines is that small and medium-sized businesses increasingly know they need to protect their files and data. But here's something you won't see in the headlines: The shadowy hackers moving through the "dark web" aren't your biggest data security risks. The biggest risks are employees—and studies show that executives and high-ranking staff are often the biggest liabilities. Humans make mistakes, we forget, we get impatient—and these flaws lead to 1 in 3 data loss incidents in the business world.[2]

CrashPlan for Small Business is offering this simple guide to help you navigate the often-murky waters of backup. We've tapped small business leaders and IT pros to uncover the features and functionalities that protect against the often-overlooked flaws of your employees, so you can build a backup and data protection strategy that perfectly fits the imperfections of the humans that drive your business.

"Day-to-day, malware isn't really the biggest threat; the biggest threat is the unintentional move or delete—the 'oops' moments. About 98% of our restores are from user error."

Michael Luehr, IT Consultant,
7 Layer IT Solutions

1 Verizon 2017 Data Breach Investigations Report
2 Egress Software Technologies 2016

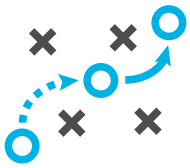
Why we're our own worst enemy

How do employees cause data loss incidents? By being human.

- **Humans forget:**
  Employees forget to save files—plain and simple. And when they do save files to their computer, they often forget to back up those files to the server or network drive.

> "Lesson learned: You can talk about policy and why we should do certain things, but until something actually happens, it's hard to get people to take things seriously."
>
> **Marc Zuckerman, Producer, Timeless Travel Trailers**

- **Humans make mistakes:**
  Leaving a laptop on a plane, spilling a cup of coffee, even just mistakenly deleting or saving over a file—employees are remarkably creative in the mistakes they make.



- **Humans take the path of least resistance**:
  A knack for finding the "easy route" makes employees efficient, innovative and productive. But convenience and expediency tend to come before official policies—like where to save and when to back up files. Three in five employees admit to ignoring policy in the name of productivity; the remaining two may just be less honest about it.[3]

- **Humans want ownership:**
  About 80 percent of the typical company's value is wrapped up in its files and data.[4] Employees want to take ownership of this value—they're proud of the work they've done for your business. But sometimes, this can hurt you: They take files to help them get a new job; they take files to use in their next job; and sometimes, they even outright sell valuable files and data. Whatever the intent, 60 percent of employees admit to taking data with them when they leave.[5]

3 2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-millenial-survey-2016-exec-summary
4 dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach
5 deloitte.wsj.com/cio/files/2016/04/2688954-Insider-Threat_4

5 Keys to Building a Perfect Backup Strategy for Imperfect Humans

1. Have a Backup:

The Common Mistake: Most companies think they have their files and data backed up, but a recent study found that 58 percent of small businesses were not prepared for a data loss incident.[6] Moreover, more than half of all backups (60%) ultimately fail to effectively restore the lost files, leaving the business starting from scratch.[7]

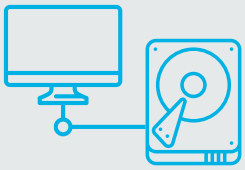
> "You should back up your data—period. And yet most businesses don't back up at all."
>
> **William Kisse, Principal, Washington Open MRI**

Backup Best Practice:

It's worth saying out loud: Any backup is better than no backup. And make sure you're following the basic "3-2-1" protocol:

3 **Keep at least THREE copies of your data:** The original, plus two backups.

2 **Spread your backups across at least TWO different types of storage (e.g., internal hard drive, removable drive, external drive, server, cloud):** Odds are much better that a technology failure will only impact one storage medium.



1 **Make sure ONE of those backups is offsite**: If all backups are kept in one place, a disaster could destroy them all.

6 clutch.co/cloud/resources/world-backup-day-2017

7 media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches

2. Make it Automatic: Not Human-Dependent

The Common Mistake: Most companies think a lot about the backup itself: where it's located, how it's protected, etc. But what about how files and data get to the backup destination? Ironically, the traditional approach is to rely on employees to manually save important files to a server, a network drive or other designated backup location. But if the biggest reason for backup is to protect against human mistakes, you can't have a backup policy that depends on those same mistake-prone humans. And think about this: Best practice is to save all files to the backup destination every 15 minutes. If your employees really did this, stopping to manually save files 32 times a day, you'd see a major drop in productivity.

Backup Best Practice:

All leading business backup solutions now automatically and silently back up files continuously. You're not vulnerable to employees forgetting to back up—and you aren't burdening your employees with the constant, productivity-draining task of manual backup.

"Any backup worth its weight should be automatic and seamless. You shouldn't have to think about it."

Marc Zuckerman, Producer, Timeless Travel Trailers

3. Back Up at the Source: Direct from the Laptop or Desktop

The Common Mistake: Research suggests 60 percent of your business' files and data live exclusively on your employees' desktops and laptops.[8] If you're only backing up a central destination like a network drive, all these work-in-progress files—all this productivity and value—are sitting on your employees' laptops and desktops, not backed up. That's because employees typically only move files to the central destination when they're finished—or at least in a "ready to share" state.

Backup Best Practice:

Since the majority of your business' files and data now live on your employees' desktops and laptops (where they do most of their work), leading business backup products pull files and data directly from these endpoint devices. This approach ensures business continuity, capturing and protecting all your employees' productivity and value.

"My guess is [if not backing up individual employee computers with an automated cloud solution] we would have paid $25,000 to recover from the ransomware attack, including time recovering files with IT consultant help, new hardware, server total loss, cost for time and materials of restoring server and productivity loss from projects we were working on with clients."

Marc Zuckerman, Producer, Timeless Travel Trailers

8 media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches

4. Get the Automatic Cloud Advantage: Unlimited, More Secure & More Cost-Effective

The Common Mistake: Another irony of traditional backup: Many companies still rely on hardware-based backup. Hardware has two big flaws: it fails, and it's vulnerable to physical damage. Moreover, conventional, on-premises backup has all the shortcomings of conventional IT: A big capital investment up front; a lengthy implementation period; and someone to manage and maintain its finite space.

> "As a small law firm, it is important to me that my files are not only secure, but my backup plan is affordable."
>
> **Joseph McLaughlin, Attorney**

Backup Best Practice:

By 2020, 4 in 5 small businesses will use automated cloud backup.[9] The cloud's multiple redundancies mean you're never vulnerable to disaster or technology failure. Automatic cloud backup is simple—instantly up and running, with nothing to manage or maintain. Data security experts agree the cloud offers the most advanced security tools, thanks to real-time updates that include the latest security patches and new security features.

Finally, cloud storage provides a cost-effective option for unlimited backup, so you don't have to choose which files to back up. This means you can follow another backup best practice: backing up every version of every file, so you can instantly go back to the moment before an incident, restoring a "clean" version and minimizing lost productivity.

> "Here's what small businesses need: automatic backup with versioning—the ability to restore any version of any file."
>
> **William Kisse, Principal, Washington Open MRI**

9 clutch.co/cloud/resources/world-backup-day-2017

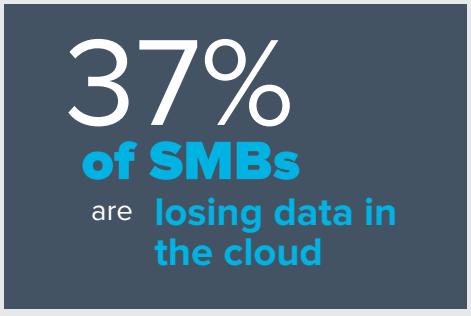
5. Cloud Sharing Apps are NOT the Same as Automatic Cloud Backup

The Common Mistake: All cloud storage apps are not created equal. Cloud sharing apps like Dropbox, Google Drive and Microsoft OneDrive are helping businesses of all sizes work in smart new ways. But, the same features that make cloud sharing apps great for sharing and collaboration make them a dangerous liability when used in place of real automatic cloud backup services:

- Depends on manual actions: Employees actively select files to add.
- Not all files are backed up: Employees only share files in the later stages of completion. All the work that went into a "shareable" draft is vulnerable to total loss.
- One person's mistakes become everyone's: If one employee makes a mistake or deletes a file—and doesn't catch it immediately—that mistake becomes everyone's problem.
- Can spread malware and ransomware: If one employee shares an infected file, it can quickly spread to everyone.
- Not designed for easy, fast file restores: If several files—or an entire laptop—are lost, the disaster recovery process typically requires a time-consuming restore.

Backup Best Practice:

With 37% of SMBs losing data in the cloud,[10] it's no surprise that data security experts and analysts agree: true backup is a critical complement to cloud-sharing apps. Dedicated backup products plug the gaps left by cloud sharing apps, ensuring continuous data protection of all files. True backup products are also purpose-built for the fastest disaster recovery, organizing files for quick restores and offering point-in-time restore. The bottom line: Cloud-sharing apps are designed to push work forward; true backup is purpose-built to allow you to bounce back.



"OneDrive is great for being able to share data outside of the organization (large files), but at the end of the day, it doesn't protect the entire computer. That's where the CrashPlan software comes into play because it does protect the whole computer."

Michael Luehr, IT Consultant, 7 Layer IT Solutions

10 Symantec 2013 Report "Avoiding the Hidden Costs of the Cloud"

What Are Your Compliance Requirements?

Small businesses face an increasing range of data security, data privacy and data protection regulations, such as PCI, HIPAA, GDPR, GLBA, SEC standards, and more. In many ways, these regulations address the same problem as data backup: protecting sensitive information from erroneous humans. And because business backup often plays a critical role in meeting these compliance requirements, make sure the product you choose can fully and easily support your business' unique compliance requirements.

Keep Your People—and Your Business—Moving Forward

All the big-name data breaches and scary cybersecurity issues in the headlines have jumpstarted the data protection conversation in many organizations. But as you craft a better strategy for backup and data protection, remember this: It's still your people that play the biggest role in moving your business forward—or holding it back. Rather than building a backup strategy solely focused on hackers and cyberthreats, best practice is to take a holistic and honest approach that accounts for your employees' natural (and human) tendencies. Seek out tools that empower them—not burden them. Build a backup strategy that's silent, automatic, constant and comprehensive—and keep your people (and your business) moving forward.

Curious about what automated cloud backup can do for you? Click here to try CrashPlan for Small Business for a free month-long trial.

Simple pricing at just $10/month per device with no hidden fees. No long-term commitments or contracts.

FOR MORE INFORMATION: CRASHPLAN.COM

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CRASHPLAN.COM