CRASHPLAN
For Small Business

CYBERSECURITY FOR SMALL BUSINESS: **Disaster Recovery Plan Roadmap**

How automatic backup delivers guaranteed business data protection and recovery—no matter the threat

The Full Cost of Small Business Ransomware

The epidemic of small business ransomware offers an even quicker payday for data thieves. Ransomware quietly installs on a victim's device and mounts an extortion attack—demanding a ransom in return for your data. Ransomware is running rampant across the business world: attacks grew by 600 percent in 2016, more than $1 billion in ransom payments and untold billions in extended damage.[1] Two in five small businesses have already been hit with ransomware.[2]

When ransomware hits, the average small business experiences two full days of downtime.[3] One-third of businesses lose revenue and all experience brand and loyalty damage that's harder to quantify.[4] To stop the bleeding, most small businesses end up paying at least $2,500 to get their data back.[5] But paying the ransom doesn't guarantee anything. Plenty of businesses have fully complied with the ransom demands, only to have the ransomer increase the ransom request—or simply take off with the ransom *and* the data.

Small Businesses Face More Attacks, More Devastating Consequences

As big-name corporate data breaches and high-profile enterprise hacks make daily headlines, the same sophisticated attacks are increasingly hitting smaller targets: small to medium-sized businesses that often lack the automatic backup strategy their larger peers employ. Nearly half (43%) of all cyberattacks now target organizations with 250 employees or fewer.[6] And reports suggest there's a one-in-two chance your small business will be hit with some form of cyberattack in the next 12 months.[7]

It's a big threat—with dire consequences. The average attack costs a small business more than $20,000.[8] Buried by these costs, 60 percent of small businesses shut down permanently within a year of an attack.[9]

CYBERATTACK HAS DEVASTATING IMPACTS

The average attack costs an SMB

$20,000

3 in 5

SMBs shut down permanently within one year of an attack

Source: sec.gov, U.S. National Cybersecurity Alliance

IT PAYS TO HAVE GUARANTEED RECOVERY

Fast, complete recovery of deleted files, corrupted drives and other restore situations could save an SMB

$2,000/week

An SMB could save

$10,000

with guaranteed recovery after a ransomware attack

$$$

Source: David Pells, System Integrator, Cyber-Wise

It's Data Loss You Should Worry About

For a small business, the biggest threat isn't the breach; it's losing your data. Losing critical data like customer information, financial account information or intellectual property—or even temporarily losing access to that data—leads to devastating costs:

- **Downtime:** Losing data/files that are essential to your business can mean complete downtime. For example, most small businesses hit with ransomware are down for two full days.[10] Unplanned downtime costs a small business as much as $8,600 an hour.[11]
- **Lost productivity:** Almost 80 percent of downtime costs come from lost employee productivity.[12] Your employees can't do their day-to-day work because they can't access their files.
- **Recreating lost work:** If files can't be recovered, you're stuck with the cost of recreating them.
- **Missed sales opportunities:** It's a fast-paced, no-apologies world. If your sales team can't give a presentation because the pitch deck is lost, that opportunity might be gone for good.
- **Lost revenue:** Downtime, lost productivity, missed sales opportunities—these all hit your bottom line, hard.
- **Brand/customer loyalty damage:** For smaller companies, downtime and reduced service levels can deliver a hit to customer loyalty and brand reputation—something many never recover from.

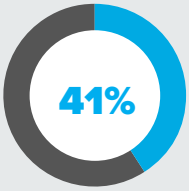
Outdated Technologies Fail to Protect Small Businesses

Cybercriminals know smaller organizations have fewer resources to dedicate to data security, making them an easier target. Compromising just one user often grants the "keys to the castle." Put another way, just one simple click on an infected email or malicious link and the entire company is in trouble.

Traditional security tools—conventional user authentication, firewalls, antivirus products—struggle to keep pace with rapidly evolving threats and cyberattack tactics. For example, antivirus products can hardly keep up with the thousands of malware strains born every day. Traditional security tools also can't fight today's sophisticated social engineering tactics—they're nearly useless if you or your authorized users are the ones unknowingly launching the attack on your business.

Most concerning of all, two in five small businesses don't practice regular data backups, meaning they have no choice but to pay data ransomers and face the full costs of data loss.[13]

CYBERATTACK IS THE TOP THREAT FACING SMBS



41% of surveyed small business customers find that ransomware, phishing attacks, and other viruses are the top threat to their business data.

Source: Tech Validate

4 Steps to Cyberattack Recovery: A Disaster Recovery Plan Roadmap

1 Back Up Every Device—Every Device Matters

Most businesses—of every size—have relied on a central server or network drive to backup all their critical data and information: Save files to the server, then backup that server in another location. This two-step process is unnecessarily complicated and leaves an immense blind spot: all your employees' laptops and desktops. Around 60 percent of all small business data lives on desktops and laptops.[14] If you want to ensure every file is covered, then you need a solution that automatically backs up data directly from every laptop and desktop—Windows, Mac and Linux. This eliminates both the hassle and the risk that not all files will be saved to a network drive.

2 Tap The Benefits of Cloud Backup

Tape-based backup, external hard drives, on-site servers—they're all easily damaged, can fail unexpectedly and can even be stolen. If backup is meant to protect you from the unexpected why back up to a medium that's vulnerable to disaster? Cloud backup has emerged as the most secure option for business backup, providing extensive redundancies guarantees continuous availability—it's virtually disaster-proof. The cloud also offers the most advanced data security capabilities, including sophisticated, end-to-end encryption that protects your data as it moves from your laptops and desktops to the cloud backup. Finally, the cloud enables leading backup providers to offer truly unlimited backup, meaning you can protect every version of every file, forever—so you're always ready for fast recovery of any information.

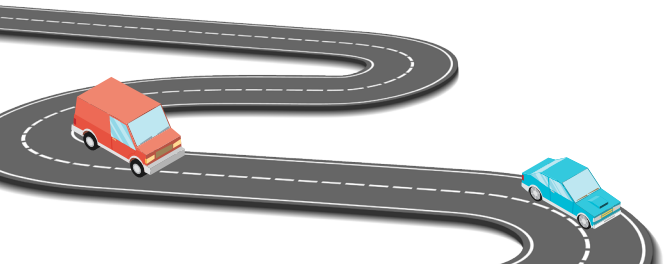
3 Ensure You Have Automatic Backup

You know your employees don't follow IT policies—you probably don't all the time, either. If a policy is inconvenient, people will find ways to work around it. Manually backing up data is a big inconvenience. It's a hassle to stop what you're doing to back up—moreover, backup is meant to protect against the unexpected: accidents, mistakes, disasters and the unpredictable. Humans have accidents, make mistakes and are unpredictable. Employees forget or choose not to regularly back up. That's why an effective business backup strategy can't depend on any manual activity. Your disaster recovery plan should start with backup that's automatic and continuous. Automatic backup gives you certainty that every version of every file is always backed up and recoverable—without frustrating your employees and impeding productivity.

4 Prioritize Faster Recovery

Most businesses don't think much about file restores until they're forced to. But what good is great backup if you can't restore quickly and completely? Most companies discover the shortcomings of their restore capabilities the hard way: tedious searching for lost files in unorganized data stores, painstaking file-by-file restores and corrupt backups that leave them starting from scratch.

Recovery should be the top priority for your backup solution. It should be purpose-built to give you the fastest restores. Features like global data deduplication can speed restores up to nine times faster. You should be able to execute point-in-time restores—of an entire device—to the moment before an attack. You and your employees should be able to restore files on your own—no waiting for an IT specialist. You should be able to recover files to any device—laptops, desktops and tablets; Mac, Windows or Android—and you should be able to do it from home or on the road, without needing a VPN connection.



SMB Cybersecurity Starts with a Comprehensive Data Loss Prevention and Disaster Recovery Plan

Never lose your data. Never pay the ransom. Minimize downtime. Get back to business quickly and successfully.

These are the goals that guide forward-thinking small organizations as they develop their data loss prevention and disaster recovery plans. Fortunately, with the right backup solution in place—delivering automatic backup and guaranteed recovery of all files, directly to and from the laptops and desktops where productivity happens—you can gain the peace of mind that your most valuable assets are always protected.

See Automatic Backup in Action—Request Your Free Trial

See how CrashPlan for Small Business checks every box in your disaster recovery plan checklist. It delivers unlimited storage and automatic cloud backup that is simple to use and affordable at just $10/month/device—with no hidden costs. Request your free trial today.

Make Recovery Quick and Easy

EVERY FILE—GUARANTEED

Automatic, continuous endpoint backup

TURN BACK THE CLOCK

Point-in-time restores

DO IT YOURSELF

Simple self-restore capabilities

ANYTIME, ANYWHERE

Cloud-based remote restore capabilities

BUILT FOR SPEED

Global deduplication at the source to speed restores up to nine times over

[1] phishme.com/malware-year-in-review-2016
[2] Ponemon Institute: The Rise of Ransomware
[3] prnewswire.com/news-releases/report-identifies-ransomwares-biggest-cost-to-be-business-downtime-300236505.html
[4] go.malwarebytes.com/OstermanRansomwareSurvey.html?utm_source=blog&utm_medium=social
[5] Ponemon Institute: The Rise of Ransomware
[6] symantec.com/security-center/threat-report
[7] signup.keepersecurity.com/state-of-smb-cybersecurity-report
[8] sec.gov/news/statement/cybersecurity-challenges-for-small-mid-size-businesses.html
[9] U.S. National Cyber Security Alliance; www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business
[10] prnewswire.com/news-releases/report-identifies-ransomwares-biggest-cost-to-be-business-downtime-300236505.html
[11] v1.aberdeen.com/launch/report/research_report/9311-RR-SMB-cloud-backup.asp
[12] dataresolution.net/true-cost-downtime-2016/
[13] Diffusion Group Study
[14] media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

FOR MORE INFORMATION: CRASHPLAN.COM

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