CRASHPLAN
For Small Business

SMB Data Loss:

WHY IT'S A THREAT AND STRATEGIES TO MANAGE BUSINESS RISKS

Executive Summary

With data making up the foundations of today's companies, any loss or downtime incident can have serious consequences for a small business.

Although backup strategies continue to improve – moving away from physical storage towards the cloud – even these more advanced solutions fail to prevent data loss through common issues such as accidental overwrites and other user errors.

While SMBs were previously regarded as too small and unimportant to be targeted by hackers, their consequent failure to recognize the value of their data and invest in appropriate IT resources and training means that they are now overrepresented in cyberattacks. Furthermore, when SMBs suffer data loss incidents, they are disproportionately affected by the impacts of downtime, lost revenue and damaged brand reputation compared to larger businesses.

ALTOGETHER, THE QUESTION IS NOT IF, BUT WHEN DATA LOSS INCIDENTS WILL OCCUR. Accordingly, it is vital for SMBs that they plan a secure data protection strategy to safeguard their business.

37% of SMBs have reported losing data saved in the cloud[1]

Only 22% of small business employees reported that their company compelled its staff to use a password manager[2]

66% of SMBs reported that a data loss incident would cause them to shut down for at least a day, or even put them out of business altogether[3]

39% of SMBs admitted that they would be prepared to hand over "almost any price" if they suffered a ransomware attack[4]

Current state of the industry:

VALUE OF DATA

With the creation and use of data being at the core of most businesses – from customer information to intellectual property to financial reports and projections – any significant loss of this information can have a critical impact. THIS ESSENTIAL ASSET IS CONSTANTLY AT RISK FROM DANGERS AS DIVERSE AS

RANSOMWARE, HARDWARE FAILURE, USER MISTAKES OR EVEN NATURAL DISASTERS.

Regardless of the cause, data loss can be incredibly costly – especially for small businesses. Sums demanded in a ransomware attack, for example, average $4,200 USD per user at a small company.[5] In addition, the damage data loss causes a company extends far beyond the alarming headlines of cash payments paid to cybercriminals.

BACKING UP FILES

When it comes to protecting important files, businesses have customarily depended on creating backups that can be retrieved should they experience a data loss incident. Because backups made to physical hard drives stored in the same location leave data at risk of being wiped out entirely by natural disasters, theft, or other location-based incidents, cloud-based solutions are becoming the new norm.

This often leads businesses to turn to cloud storage and cloud collaboration tools like DropBox and OneDrive. While they are cloud-based, these file sharing and collaboration tools should not be viewed as a solution for protecting valuable company data. Using them to store files is dependent on employees proactively saving their work to a designated location, a step that is all too easy for users to forget. In addition, accidental overwrites and user errors – the most frequent cause of cloud data loss in the workplace[6] – remain a problem. And, when an SMB is hit with a virus or malware attack, the malicious software is quickly spread throughout the organization via the cloud. Unsurprisingly, 37% of SMBs have reported losing data saved in the cloud.[7]

ALONGSIDE RELIABILITY IS THE ISSUE OF COVERAGE.

Since small business employees increasingly use a variety of personal laptops and other private devices for day-to-day tasks, cloud collaboration tools that only copy files from a folder on company-owned device risk missing key files.

EVOLUTION OF RISKS OF DATA LOSS TO SMBS

As data has grown rapidly in value in recent years, SMBs are increasingly viewed by cyber criminals as a valuable and often-exposed source of corporate and personal information.

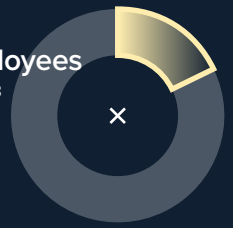
In the past, SMBs' relative lack of capital and lower public profile meant that they were frequently spared from the bulk of advanced cyberattacks.[8] UNFORTUNATELY, THE COMBINATION OF ASSUMING THAT THEY ARE UNATTRACTIVE TO CRIMINALS ALONG WITH THEIR LESS-SOPHISTICATED IT RESOURCES HAS SEEN THEM BECOME A PRIME TARGET FOR ATTACKS.

58% of companies that suffer cyberattacks today are classified as small businesses.[9] For ransomware, this figure rises to 71%.[10]

SMBS ARE FALLING BEHIND

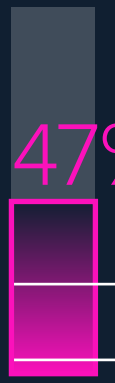
SMBs' limited IT budgets and failure to recognize their increasing vulnerability has led to many neglecting to properly invest in IT security, and consequently seeing themselves fall further behind better-prepared larger businesses.[11] This gap in IT skills and resources means that smaller businesses are left to rely upon their employees' own confined understanding of cybersecurity.[12]

Only 18% of SMBs in the United States provide employees with regular IT training in order to help prevent cybercrime.[13]



Established password policies, for example, are a common weak point for SMBs: Only 22% of small business employees reported that their company compelled its staff to use a password manager. Likewise, 67% of employers agreed that personnel using weak passwords was a considerable burden to their business,[14] leaving them vulnerable to ransomware attacks.

Number and increased frequency of attacks



47% of small businesses in the US and a number of European countries were victims of a cyberattack between 2017 and 2018.[15] Among these victims, 44% had been exposed to 2 to 4 attacks during that period, while 8% had suffered 5 or more.[16]

In 2018, incidents among small businesses rose year-over-year by 59%, averaging 62 per day.[17]

98% of SMB owners reported that cybercrime was a threat to their businesses, with 25% and 46% reporting that they saw it as a major or moderate threat respectively.[18]

REMOTE WORK AND THE RISK OF DATA LOSS

The growth of remote work is particularly relevant to smaller businesses, who benefit from the increased flexibility and easier engagement with freelancers. With 99% of respondents to a 2019 Buffer survey revealing that they wish to work outside of the office at some point during the remainder of their career,[19] remote work is a trend that will be at the core of SMBs' business model for the foreseeable future.

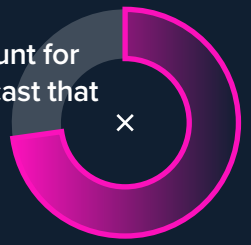
WITH THE GROWING POPULARITY OF REMOTE WORK, IT PRESENTS A RANGE OF

NEW CHALLENGES FOR BUSINESS' DATA SECURITY.

On a practical level, for example, remote work inevitably leads to a rise in employees losing work devices or other company property. Loss of portable devices is responsible for almost as many data loss incidents as hacking or malware.[20] And the problem is not going away anytime soon.

With Millennial and Gen Z employees expected to account for more than half of the workforce in 2028 (58%), it is forecast that

73% of teams will include remote staff.[21]



THE POTENTIAL IMPACT OF DATA LOSS INCIDENTS ON SMBS

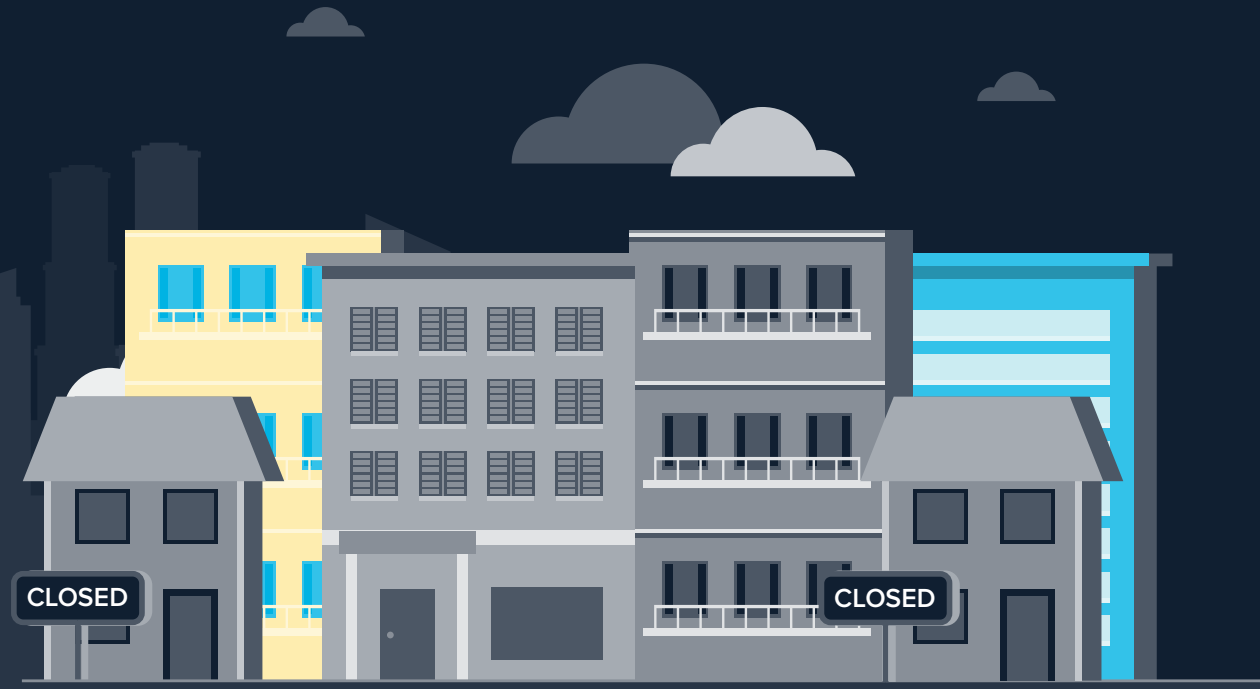
In spite of the fundamental role reliable access to key data has in the modern workplace, SMBs are frequently guilty of not fully considering the impact of staff being locked out of their files when developing data protection policies.

In fact, when small businesses experience data loss, 80% of costs can be attributed to the decrease in employee productivity.[22] A single hour of downtime can cost SMBs as much as $8,600 USD, while an outage lasting a whole day can cause damages of up to $68,800 USD.[23]

As a result, 66% of SMBs reported that a data loss incident would cause them to shut down for at least a day, or even put them out of business altogether.[24] While the standing of any company can be damaged by a data loss emergency, SMBs' size means that they are disproportionately affected by downtime and lost revenue. Furthermore, since they have a less-established reputation in the first place, many never regain clients' trust following the hit to their brand image.[25]

And because of their more limited resources, SMBs are especially vulnerable to being exploited in ransomware attacks. If their data was held hostage by cybercriminals, 55% of small businesses reported that they would be willing to pay to get their files back, a figure that rises to 74% among larger SMBs. Almost four out of ten (39%) admitted that they would be prepared to hand over "almost any price" in such an event.[26]

Unfortunately, among SMBs that do pay a ransom following an attack, almost one in five (18%) never recover their data. Furthermore, fewer than 33% of incidents suffered by SMBs are reported to the authorities.[27]



Protecting data in an increasingly dangerous climate for SMBs

RECOMMENDATIONS

Ultimately, for SMBs, the issue doesn't come down to if they experience a damaging data loss incident, rather a matter of when one will happen.

As has become clear, with preventative security solutions only be able to limit the risks to small businesses while attacks are continually becoming more advanced, the focus needs to shift to the protection of data.

The data protection approach recognizes the constant dangers to SMBs and, instead of relying upon daily backups to an in-office server or hard drive, copies data to the cloud automatically as frequently as every half hour. This ensures that, regardless of whether systems are affected by ransomware, physical damage, hardware failure or, very frequently, user mistakes, no more than 30 minutes of a business' work will be lost.[28]

By storing data in the cloud, files are physically safe from day-to-day physical or technology-related disasters, while also ensuring that backups can be accessed easily from outside the office – a solution tailor-made for the modern, flexible workplace.

A data protection-focused strategy addresses SMBs' limited IT security resources by ensuring that backup and recovery is user-friendly and efficient. Since backups are made automatically, smart security practices are no longer dependent on user behavior or work style preferences. Cloud-based data protection systems are designed to be deployed easily in a day or two, while a fast, self-service restoration means that a company's up-to-date files can be retrieved without the help of IT.

Ultimately, protection against data loss, regardless of cause, will require a multi-pronged approach including user training and education, local backups for quick restores when hardware is lost or damaged, and a cloud-based backup solution to protect against outside threats such as ransomware, theft, or extreme weather event.

Endnotes

1 “The Perfect Guide to Data Loss Protection”, www.crashplan.com, July 2019

2 “2018 State of Cybersecurity in Small & Medium Size Businesses”, www.keepersecurity.com, November 2018

3 “VIPRE Announces Launch of VIPRE Endpoint Security – Cloud Edition”, www.businesswire.com, October 2017

4 “Majority of SMB Leaders Say They Would Pay Ransom to Have Stolen Data Returned” www.appriver.com, April 2019

5 “The Cost of Data Loss to Your Small Business”, www.avg.com, June 2018

6 “2019 Global Encryption Trends Study”, www.ncipher.com, August 2019

7 “The Perfect Guide to Data Loss Protection”, www.crashplan.com, July 2019

8 “Why Your Business Might Be a Perfect Target for Hackers”, www.inc.com, December 2014

9 “2019 Data Breach Investigations Report”, www.enterprise.verizon.com, July 2019

10 “71% of Ransomware Attacks Targeted Small Businesses in 2018”, www.healthitsecurity.com, March 2019

11 “The Most Effective Ways to Protect Your Small Businesses From Cyber Attacks”, www.smallbiztrends.com, January 2019

12 “3 Reasons Why Hackers Like to Target Small Businesses”, www.pacetechnical.com, August 2019

13 “U.S. SME Protections Against Cybercrime 2016”, www.statista.com, October 2016

14 “2018 State of Cybersecurity in Small & Medium Size Businesses”, www.keepersecurity.com, November 2018

15 “2018 HISCOX Small Business Cyber Risk Report”, www.hiscox.com, January 2018

16 “2018 HISCOX Small Business Cyber Risk Report”, www.hiscox.com, January 2018

17 “SiteLock 2019 Website Security Report”, www.sitelock.com, August 2019

18 “Risk of Cybercrime to SMEs in the U.S. 2016”. www.statista.com, October 2016

19 “State of Remote Work”, www.buffer.com, August 2019

20 “Follow the Data: Dissecting Data Breaches and Debunking Myths”, www.trendmicro.com, July 2019

21 “Third Annual ‘Future Workforce Report’ Sheds Light on How Younger Generations are Reshaping the Future of Work”, www.upwork.com, March 2019

22 “Business Continuity: Understand Your Risks from Data Loss”, www.crashplan.com, July 2019

23 “Report Identifies Ransomware’s Biggest Cost to be Business Downtime”, www.prnewswire.com, March 2016

24 “VIPRE Announces Launch of VIPRE Endpoint Security – Cloud Edition”, www.businesswire.com, October 2017

25 “Business Continuity: Understand Your Risks from Data Loss”, www.crashplan.com, July 2019

26 “Majority of SMB Leaders Say They Would Pay Ransom to Have Stolen Data Returned”, www.appriver.com, April 2019

27 “Datto’s State of the Channel Ransomware Report EUROPE”, www.datto.com, August 2019

28 “What Does Data Loss Protection Mean for Small Business?”, www.crashplan.com, June 2019

About Us

CrashPlan® for Small Business is a product of Code42, an industry leader in data security, protecting the critical data of more than 50,000 world-class organizations, including the largest global brands. Hosted on Code 42's enterprise-grade secure cloud system, CrashPlan for Small Business' automatic backup solution is specifically designed to meet the needs of SMBs. We help small businesses and organizations recover and bounce back faster from data loss incidents, whether caused by natural disaster, simple human error, a stolen laptop, ransomware and more.

CrashPlan® for Small Business provides peace of mind through easy-to-use, unlimited automatic data loss protection. In the event of an incident, CrashPlan's automated data protection reduces the amount of potential lost work to as little as 30 minutes. And restoration of user data can even be done by users themselves – limiting the burden on IT. Signup is fast and easy, and you'll enjoy peace of mind knowing your data – and your business – is protected. Use this link to get started protecting your business with CrashPlan for Small Business.

CRASHPLAN
For Small Business