Let's talk about data loss

Breaking down why your data needs backing up

Let's talk about data loss

Breaking down why your data needs backing up

It's all too easy to put off getting a backup solution — until it's too late and your business data has disappeared. Despite the proven pain of data loss, many small- to medium-sized businesses (SMBs) continue to question if they really have a need for backup.

Don't become another statistic!

"It won't happen to us"

Based on current rates, it's a coin toss whether you'll experience a data breach or get hit by a ransomware attack in the next year.

In 2021, more than a third of organizations globally suffered an attempted ransomware attack.[1]

66% of senior decision-makers at SMBs do not believe they are likely to be targeted by cyberattacks.[2]

"We're too small to be targeted for a cyberattack"

Attackers see SMBs as softer targets than enterprises, as they have fewer security resources, less sophisticated defenses, and are more inclined to pay ransoms because they simply can't afford the downtime.

46% of all cyber breaches impact businesses with fewer than 1,000 employees.[3]

68% of SMBs experienced a serious cloud security incident in 2022.[4]

"We don't have anything hackers want"

If you run a business, you have information that attackers want. From customer/employee records to proprietary information, your data has value to criminals and competitors.

57% of SMBs say customer records are their biggest data loss concern and 51% say intellectual property.[5]

When it comes to ransomware, attackers don't care about the resale value of your data. They just need to hold it hostage so that you'll pay to get it back.

"We have antivirus software in place"

Installing antivirus software and email filters is simply no longer enough to protect your business in the face of today's sophisticated attacks.

59% of ransomware victims had anti-malware filtering, and 42% had legacy signature-based antivirus installed.[6]

72% of victims say exploits and malware evaded intrusion detection systems, 82% say they evaded antivirus solutions.[5]

"I'm not convinced. I just really don't think we're a target for a cyberattack"

Even if your business is lucky enough to never face a cyberattack, there are a multitude of other ways you can lose valuable data and most of them start with simple user mistakes.

88% of today's data breaches are caused by human error.[7]

In other words... the #1 cause of data loss is human error – deleting files, opening phishing emails, accidentally downloading malware, etc.[7]

"Most of our data is in the cloud... so that means we're safe, right?"

SaaS applications are still vulnerable to data loss because human error is the main cause of data loss.

45% of breaches were cloud-based.[8]

38% of business leaders ranked SaaS applications and 36% ranked cloud-based storage as the main targets of cyberattacks.[9]

"Microsoft stores our data, right? So we'll be able to get it back"

Deleted data is only retained for 14 days in Exchange, 30 days in O365 Groups, and 180 days in SharePoint/OneDrive for Business. Data can't be restored past the retention date.

Microsoft recommends the use of a third-party backup solution in their Microsoft Services Agreement.

By now, it's pretty clear that no business is immune to data loss. When it happens, it hurts.

Record Loss

Businesses lost an average of 10,848 individual records over the past 12 months.[5]

Cost of a breach

Average cost of a data breach for a company with fewer than 500 employees in $3.31M.[9]

Cost per breached record

Average cost per breach record is $164.[9]

Compliance fines

Fines can be as much as 4% of a company's total revenue.[10]

Cost per attack

95% of cybersecurity incidents at SMBs cost between $826 and $653,587.[3]

Downtime

50% of SMBs report that it took 24 hours or longer to recover from an attack.[11]

Downtime cost

Lost data due to mission-critical app downtime costs $102,450/hour on average.[12]

Impact of outage

54% of businesses with an outage experienced loss of customer confidence, 38% damage to brand integrity, and 37% loss of employee confidence.[12]

Impact on operation

75% of surveyed SMBs say they would survive only three to seven days after a ransomware attack.[13]

So what can you do?

While implementing a comprehensive, layered security strategy can be a complex undertaking, the simplest first step you can take to mitigate the threat of data loss is to start using a third-party backup solution. Having a full backup of your data makes recovering from a data loss incident much easier.

Don't become another data loss statistic.

Let Pax8 help you find the right backup solution for your business needs.

Sources

1. AAG, The Latest 2023 Ransomware Statistics, 2023

2. Keeper Security, 2019 SMB Cyberthreat Study

3. Verizon, SMB Data Breach Statistics, 2021

4. Snyk, The 2022 State of Cloud Security Report, 2022

5. Ponemon Institute, 2018 State of Cybersecurity in Small & Medium Size Businesses

6. Datto, 2020 Global State of the Channel Ransomware Report

7. Tessian, The Psychology of Human Error, 2022

8. Thales, 2023 Cloud Security Study, 2023

9. IBM, 2023 Cost of a Data Breach Report, 2023

10. Skykick, Protect Your Office 365 Experience with Cloud Backup, 2019

11. BullGuard, New Study Reveals One In Three SMBs Use Free Consumer Cybersecurity And One In Five Use No Endpoint Security At All, 2020

12. Veeam, 2019 Cloud Data Management Report, 2019

13. CyberCatch, Small and Medium-Sized Businesses Ransomware Survey, 2022