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 enterprises (SMEs) continue to stick their heads in the sand when thinking about the need for backup.

That's what they all say

Don't fall prey to these common SME fallacies!

"It won't happen to us"

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

48.5% businesses in Europe suffered a cyberattack in 2022.[1]

Cybercrime cost UK businesses an average of **£4.2k** in 2022.[2]

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

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

Phishing is the most common cyberattack in Europe.[3]

European SMEs saw a **26%** increase in cyberattacks in 2022.[4]

"We don't have anything hackers want"

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

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.

Phishing was the most common cyberattack in Europe in 2022, with an 11% increase since 2021.[5]

"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.

50% of ransomware attacks averted antivirus/ anti-malware solutions.[6]

85% businesses in Europe agree a breach would have a serious detrimental impact on their business, and **57%** said they'd likely go out of business.[7]

"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.

51% of IT leaders say human error is their organisation's biggest vulnerability, with the most likely cause being employees clicking on a malicious link or downloading a compromised file **(43%)** and falling victim to phishing emails **(39%).**[8]

85% of all data breaches involved a human element.[9]

"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.

Over **70%** of data loss in cloud apps is due to accidental or malicious deletion by end users.[10]

32% of companies lose data in the cloud: **64%** due to accidental deletion, **13%** due to hackers, **7%** due to malicious deletion, and **16%** due to software issues.[11]

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

Microsoft 365 and Office 365 only store data for 30 days, and Microsoft themselves recommend the use of a third-party backup solution in their Microsoft Services Agreement.

In 2022 it took **277 days** (approx. 9 months) to identify and report a security breach.[12]

81% of surveyed IT professionals experienced data loss in Microsoft 365 or Office 365.[13]

Sources

1. 'Share of companies in the United States and selected European countries having experienced a cyber attack as of 2022, by country', *Statista*, 27 February 2023, https://www.statista.com/statistics/1006664/european-firms-cyberattack-target-reporting/

2. 'The Latest 2023 Cyber Crime Statistics', *AAG*, August 2023, https://aag-it.com/the-latest-cyber-crime-statistics/

3. 'Phishing most common Cyber Incident faced by SMEs', *ENISA*, 28 June 2021, https://www.enisa.europa.eu/news/enisa-news/phishing-most-common-cyber-incidents-faced-by-smes

4. 'Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks', *Checkpoint*, 5 January 2023, https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

5. '20 Cyber Security Statistics for 2022', *IT Governance*, 17 February 2022, https://www.itgovernance.eu/blog/en/20-cyber-security-statistics-for-2022

6. 'Datto's Global State of the Channel Ransomware Report', *Datto*, 2020, https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf

7. 'Phishing most common Cyber Incident faced by SMEs', *ENISA*, 28 June 2021, https://www.enisa.europa.eu/news/enisa-news/phishing-most-common-cyber-incidents-faced-by-smes

8. 'People-Centric Cybersecurity: A Study of IT Leaders in the UK & Ireland', *Proofpoint*, 2021, https://www.proofpoint.com/sites/default/files/white-papers/UK_CISO-REPORT_FINAL.pdf

9. 'Data Breach Investigations Report', *Verizon*, 2021, https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

10. 'Selling SaaS Backup Made MSPeasy', *Datto*, https://www.datto.com/resource-downloads/SellingSaaSBackupMadeMSPeasyO365

11. 'The role of Cloud Backup in Office 365', *SkyKick*, 4 April 2018, https://www.skykick.com/blog/the-role-of-cloud-backup-in-office-365/#_ftn1

12. 'How long does it take to detect a cyber attack?', *CYFOR Secure*, https://cyforsecure.co.uk/how-long-does-it-take-to-detect-a-cyber-attack/#:~:text=So%2C%20how%20long%20does%20it,and%20report%20a%20data%20breach

13. 'Protect Your Business from Microsoft 365 Data Loss with Managed Backup', *Modern Networks*, 15 March 2023, https://modern-networks.co.uk/news/microsoft-365-managed-backup