Let's talk about Data Loss

Breaking down why your data needs backing up

It's easy to put off getting a backup solution for your business until it's too late and your data is gone. But despite the risks, many small and medium-sized businesses (SMBs) bury their heads in the sand.

That's what they all say

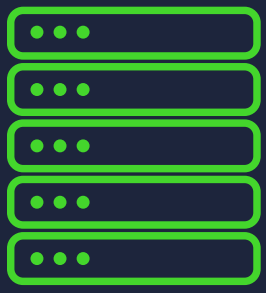
Don't fall prey to these common SMB misconceptions!

"It won't happen to us."

You're more likely to be the victim of a ransomware attack or data breach than not.

- 69% of businesses were the victim of a ransomware attack in 2021[1]
- 61% of business leaders expect ransomware incidents to increase in 2022[2]

"Our business is too small to be attacked by cybercriminals."



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

- 28% of data breach victims are small businesses[3]
- 70% of MSPs believe ransomware is the biggest malware threat to SMBs[4]

“We don’t have anything hackers want.”

If you run a business, you have data hackers want. From customer and 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; 51% say intellectual property[5]
- Ransomware attacks cost UK companies £346 million a year[6]

“We have antivirus software in place.”

Basic antivirus software and email filters are no longer enough to protect your business in todays’ complex threat landscape. Criminals will happily exploit any gaps in your defences.

- 59% of ransomware victims have anti-malware filtering[7]
- 42% have legacy signature-based antivirus[7]

“I’m not convinced. I just really don’t think we’re a target.”

Even if you get lucky and a hacker has never targeted your business, there are plenty of other ways to lose data.

- Hardware failure is the #1 cause of data loss[8]
- Human error is responsible for 29% of lost business data[8]

“Most of our data is in the cloud – that means it’s safe, right?”

SaaS applications aren’t infallible. Accidental and malicious deletion is just as much of a threat in cloud environments as it is on-premises.

- Over 70% of data loss in the cloud is a result of accidental or malicious deletion[9]
- 21% of MSPs have seen ransomware attacks in their clients’ SaaS applications[7]

“Microsoft stores our data, so we’ll be able to get it back.”

Microsoft 365 and Office 365 only store data for 30 days. The Microsoft Service Agreement recommends third-party backup solutions for this very reason.

- It takes the average business 184 days to detect a breach and 63 days to contain it[10]
- 37% of SMBs have lost data in the cloud[11]

No Business is Immune to Data Loss...
When it happens, it hurts

Financial impact: It costs the average UK enterprise £618,000 to recover from a successful ransomware attack[12]

Reputational damage: Lost business is responsible for 38% of the total costs associated with data breaches[10]

Going offline: Ransomware attacks cause an average of 22 days of downtime[13]

Downtime costs: Downtime costs are 23 times greater than the ransom amount requested[7]

Double trouble: 80% of organisations that pay a ransomware demand are hit again; almost half by the same threat group[14]

Compliance fines: The ICO can levy fines of up to £17.5 million (or 4% of annual global turnover - whichever is greater) for failing to comply with UK data protection laws[15]

Gone forever: : Victims who pay the ransom for a decryptor recover 92% of their data on average[16]

Bad publicity: 14% of companies that experience a ransomware attack report negative press and bad publicity[5]

Lost customers: 41% of UK customers will never work with a business again once it's suffered a cybersecurity breach[12]

What can you do about it?

The first step to mitigating the effects of data loss is to find the right combination of business continuity and disaster recovery (BC/DR) solutions.

We connect our partners to a range of robust BC/DR solutions supplied by leading vendors including Acronis, Axcient, Dropsuite, and Skykick. So should the worst happen, you can get your clients back up and running - fast.

Don't become another data loss statistic. Schedule a call and we'll help you find the right backup solution for your business

Sources

[1] Statista, Percentage of Organisations Victimized by Ransomware (2018-2021)
https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

[2] PWC, Two thirds of UK business leaders expect cyber security threat to increase over next 12 months
https://www.pwc.co.uk/press-room/press-releases/two-thirds-of-uk-business-leaders-expect-cyber-security-threat-t.html

[3] Verizon, Data Breach Investigations Report, 2021
https://www.verizon.com/business/resources/reports/dbir/

[4] Datto, Top Tips for MSPs: Protecting Customers from Phishing and Ransomware
https://www.datto.com/uk/blog/top-tips-for-msps-protecting-customers-from-phishing-and-ransomware

[5] Ponemon Institute, 2018 State of Cybersecurity in Small & Medium Size Businesses
https://www.ponemon.org/news-updates/news-press-releases/news/2018-state-of-smb-cybersecurity-report.html

[6] Acronis, The top 5 ransomware attacks in the UK and their hidden costs on business
https://www.acronis.com/en-gb/articles/ransomware-attacks/

[7] Datto, 2020 Global State of the Channel Ransomware Report
https://www.datto.com/uk/resources/dattos-2020-global-state-of-the-channel-ransomware-report

[8] Unitrends, What Causes Data Loss?
https://www.unitrends.com/blog/backup-what-causes-data-loss

[9] Selling SaaS Backup Made MSPeasy
https://www.datto.com/resource-downloads/SellingSaaSBackupMadeMSPeasyO365

[10] IBM, Cost of a Data Breach Report 2021
https://www.ibm.com/downloads/cas/OJDVQGRY

[11] Invenio IT, 11 Data Loss Statistics All Businesses Should Know
https://invenioit.com/continuity/data-loss-statistics/

[12] CSO Online, UK cybersecurity statistics you need to know
https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html

[13] Statista, Average Duration of Downtime After a Ransomware Attack (2021)
https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/

[14] VentureBeat, Cybereason: 80% of orgs that paid the ransom were hit again
https://venturebeat.com/2021/06/16/cybereason-80-of-orgs-that-paid-the-ransom-were-hit-again/

[15] The Information Commissioner's Office (ICO)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/penalties/

[16] Sophos, The state of ransomware 2020
https://news.sophos.com/en-us/2020/05/12/the-state-of-ransomware-2020/