Ransomware: could you recover within a week without paying?

Keep at least one backup copy that your everyday admin accounts can't delete, and restore your most critical systems from it in a timed test this quarter. Judge every other ransomware measure by whether it keeps attackers away from your backups, identity systems and hypervisors or shortens that measured restore time.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.1**	**IT and security teams in small and mid-size organizations, including those on Microsoft 365**

Latest version
sheets.einblick.dev/ransomware/

If you only do five things

1. **Keep one copy attackers can't delete.**
   Store at least one backup offline or on immutable storage. Run the backup system with admin accounts separate from those that administer the rest of the network, and require MFA to alter or destroy backups[1].
2. **Time a full restore.**
   Restore your critical systems into an isolated network at least once a year and record how long it takes. In a Sophos-commissioned survey of 2,158 victims, 55% fully recovered within a week[2].
3. **Close the usual ways in.**
   Patch VPNs and firewalls within the patching sheet's deadlines and require phishing-resistant MFA for remote access. Confirmed or suspected exploits, mostly of VPNs and firewalls, opened a third of Google's 2025 ransomware cases; stolen credentials, typically for VPN or RDP, opened 21% of those with a known entry point[3].
4. **Guard the systems that control recovery.**
   Manage domain controllers, Entra ID, backup servers and hypervisors only from dedicated admin accounts and workstations. Mandiant advises treating virtualization platforms as Tier 0 and decoupling backups from the corporate Active Directory[4].
5. **Print the plan and the phone list.**
   Keep a hard copy and an offline version of the incident plan[5], with contacts for your insurer, incident response firm, lawyer, police and data protection authority.

Test whether you could recover

1. **Which services must run first?**
   List what the business needs back in the first week, with an owner and a recovery time objective for each. CISA advises restoring from a predefined critical asset list[5].
2. **Can you reach the backups with the domain down?**
   Sign in to the backup console without any domain account. If you can't, an attacker with domain admin rights can probably reach the backups.
3. **How far back can you go?**
   Ransomware can go unnoticed for days[6], so keep versions from before the intrusion. Active Directory backups are usable only within the tombstone lifetime[7].
4. **How long does a full restore take?**
   Restore identity, the backup server and one business application end to end. Time it until users can work and compare the result with the recovery time objectives.

How ransomware attacks run now

- **Access is often handed over.** In Mandiant's 2025 investigations, 30% of ransomware intrusions began with access from an earlier compromise, up from 15% in 2024, as groups that break in pass access to groups that deploy ransomware[4].
- **Recovery systems are targets.** Mandiant saw groups delete backups from cloud storage and encrypt hypervisor datastores to stop all their virtual machines at once[4]. Google saw attackers harvest credentials from Veeam backup servers in about 10% of intrusions[3].
- **Stolen data is the main lever.** Google found suspected data theft in 77% of the ransomware intrusions it analyzed for 2025, up from 57% in 2024[3]. Europol notes that companies now cope better with losing data than with having it published[8].

Backups that survive an attack

- **Use 3-2-1 with one copy out of reach.** Keep three copies on two media types, one of them offsite and one offline or immutable. Ransomware actively targets backups[9].
- **Make deletion slow and visible.** Delay deletion requests, alert on mass deletions and retention changes and keep backups for a fixed period rather than a fixed number, so a burst of corrupted backups can't push out the clean ones[1].
- **Store keys and passwords offline.** Keep out-of-band copies of backup encryption keys[1] and of the Directory Services Restore Mode password[7].

Limit lateral movement

- **Separate admin accounts.** Use designated admin accounts only for admin work, and give every machine its own local admin password with LAPS[5].
- **Segment the network.** Put servers, backups and management interfaces in their own zones, and block SMB and RDP between workstations. CISA notes that segmentation can help contain an intrusion[5].
- **Keep domain controllers bare.** Don't use them for email or web browsing, don't install extra agents and manage privileged access to them with a PAM tool[5].

Rebuild in this order

1. **Set up a clean place to work.**
   Use new or reimaged admin workstations on an isolated network. Keep affected systems intact for the investigation.
2. **Restore identity first.**
   Restore one writable domain controller per domain in isolation, then reset admin passwords and reset the krbtgt password twice[10]. Entra Backup and Recovery, generally available since June 2026[11], rolls supported objects back up to 7 days but not hard-deleted ones[12].
3. **Rebuild the recovery tools.**
   Reinstall backup and hypervisor management from trusted media and rotate their credentials.
4. **Restore services in priority order.**
   Use golden images[5], scan backup data for malware before restoring it[9] and reconnect one zone at a time.

If you are asked to pay

- **Don't count on payment.** It doesn't guarantee access to your data, and a promise to delete stolen data can't be trusted[13]. In Verizon's 2026 DBIR, 69% of ransomware victims didn't pay and the median payment fell to $139,875[14].
- **Screen for sanctions first.** Breaching UK financial sanctions is a serious criminal offense, and OFSI says ransomware payments are unlikely to get a license[15]. EU cyber sanctions forbid making funds available to listed persons, who include people behind Conti and TrickBot[16].
- **Don't expect a lower ICO penalty.** The ICO doesn't count a ransom payment as risk mitigation or as a reason to reduce a penalty[13].
- **Watch for a UK ban.** The UK is developing a ban on payments by public sector bodies and regulated critical national infrastructure[17].
- **Record each decision.** Keep a careful record of the response and each decision, and report the attack to your insurer or broker[13].

What you can skip

- **Buying another detection product before a tested restore.** If no one has timed a full restore, spend the money and time there first.
- **Counting sync as a backup.** Cloud services often sync encrypted files over the good copies immediately, and NCSC advises against relying on several copies in one cloud service[9]. Even Microsoft 365 Backup's append-only restore points can be deleted by a Backup admin after a 90-day grace period[18]. Only cutting it to 7 days needs a second approver[19].
- **Taking every backup offline.** One offline or immutable copy of what the first week needs is enough to start. Keep the rest online for fast restores.

Mistakes that cost the most

- **Cleaning up a small infection and moving on.** Infostealers and phishing are common first steps into a ransomware attack[8]. Reset every credential used on that machine.
- **Declaring the incident over once systems are back.** Find out what was taken. Under the GDPR, a personal data breach that may put people at risk goes to the supervisory authority within 72 hours where feasible[6].
- **Rebuilding admin rights as they were.** The same broad admin groups and service accounts give the next attacker the same path. Cut them down during the rebuild.

What this looks like at your size

Small team, no security staff

- Back up OneDrive, SharePoint and Exchange Online with Microsoft 365 Backup or a third-party service, in addition to sync.
- Keep two emergency access accounts with their own MFA, and store their recovery steps on paper.
- Ask your IT provider to restore one laptop, one mailbox and one shared folder while you time it.

Growing, with IT or security staff

- Back up at least two writable domain controllers per domain[7] and practice a forest restore in isolation.
- Move backup servers and hypervisor management out of the domain and onto their own network.
- Sign an incident response retainer and check what your insurer requires before you call anyone.

Enterprise or regulated

- Keep an isolated recovery environment with its own identity, sized for the critical asset list.
- Report measured restore times per critical service to leadership against agreed targets.
- Agree with the board in advance who decides on payment, with legal and sanctions advice.

Version history

5 Nov 2026, version 1.1	Added that Microsoft 365 Backup's two-person approval covers only shortening the deletion grace period, and updated its source date.

Sources

1. Principles for ransomware-resistant on premises backups. NCSC (UK), 22 Nov 2024. ncsc.gov.uk
2. The State of Ransomware 2026 (vendor-commissioned survey, Q1 2026). Sophos, Jul 2026. assets.sophos.com
3. Ransomware Under Pressure. Google Threat Intelligence Group, 16 Mar 2026. cloud.google.com
4. M-Trends 2026. Google Cloud (Mandiant), 23 Mar 2026. cloud.google.com
5. #StopRansomware Guide. CISA, Sep 2023. cisa.gov
6. Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, version 2.0. European Data Protection Board, 14 Dec 2021. edpb.europa.eu
7. Active Directory Forest Recovery - Determine how to recover the forest. Microsoft Learn, 10 Jul 2023. learn.microsoft.com
8. Internet Organised Crime Threat Assessment (IOCTA) 2026. Europol, 28 Apr 2026. europol.europa.eu
9. Mitigating malware and ransomware attacks. NCSC (UK), reviewed 9 Sep 2021. ncsc.gov.uk
10. Active Directory Forest Recovery - Perform initial recovery. Microsoft Learn, 10 Jul 2023. learn.microsoft.com
11. Microsoft Entra Backup and Recovery is now generally available. Microsoft Entra Blog, 30 Jun 2026. techcommunity.microsoft.com
12. Microsoft Entra Backup and Recovery overview. Microsoft Learn, 30 Jun 2026. learn.microsoft.com
13. Guidance for organisations considering payment in ransomware incidents. NCSC (UK) with ABI, BIBA and IUA, 14 May 2024. ncsc.gov.uk
14. 2026 Data Breach Investigations Report: Executive Summary. Verizon, 19 May 2026. verizon.com
15. Financial sanctions guidance for ransomware. OFSI (HM Treasury), updated 28 Jan 2026. gov.uk
16. Council Regulation (EU) 2019/796 (cyber sanctions), Article 3 and Annex I, consolidated text. EUR-Lex, 13 Jul 2026. eur-lex.europa.eu
17. Ransomware legislative proposals: government response. Home Office (UK), 22 Jul 2025. assets.publishing.service.gov.uk
18. Overview of Microsoft 365 Backup. Microsoft Learn, 4 Nov 2026. learn.microsoft.com
19. Offboarding in Microsoft 365 Backup. Microsoft Learn, 1 Oct 2026. learn.microsoft.com