BUSINESS CONTINUITY BRIEFING

Plan for the day the cloud goes quiet.

EMH Technology · Eric Hughes, Managing Director · 17 November 2026

Last week's Microsoft 365 outage left many businesses without email for the best part of a working day. It is a reminder that moving to the cloud changes where your risk sits; it does not remove it. Every organisation should have a plan that covers its critical technology, the people it depends on and the processes that keep it trading.

On Thursday 12 November and into Friday 13 November 2026, Exchange Online failed for users around the world. Outlook, Outlook on the web and mobile mail apps could not reach mailboxes, and services such as Teams calendars, Copilot, Defender, Intune and Planner were also affected. Downdetector reports for Outlook peaked at around 130,000. Many of our clients asked the same question: what should we have done differently?

This time the outage was Microsoft's. The next one may be Amazon Web Services (AWS), Google or an AI platform that your staff now use every day. The advice in this article applies whichever provider fails.

Microsoft's outage holds three lessons.

Microsoft's preliminary explanation is that a defect in an update deployed to its networking gateway servers months earlier combined with higher traffic and reduced capacity. Servers became overwhelmed and failed in a cascade; at the lowest point more than 80% of gateway servers were unresponsive. Restarted servers were swamped by queued traffic, and the usual rollback tools could not help because the defect had been present for so long. Microsoft has said the incident was not caused by malicious activity.

The good news is that, according to Microsoft, email was not lost. Incoming messages were held and delivered once service recovered. Messages sent from mobile apps during the outage may not have gone, so anything important sent on 12 or 13 November is worth checking.

Three lessons stand out for every business.

- Cloud providers are very reliable, but no provider can promise that a service will never fail.
- Microsoft is responsible for restoring its platform, but you are responsible for how your business keeps working while it does.
- A single platform often carries email, calendars, chat, files and security tools together, so one fault can remove several tools at once.

The businesses that coped best last week were those that had already decided how they would communicate, who would make decisions and which work could carry on without email.

© EMH Technology Limited 2026

The next outage may not be Microsoft.

Every major provider has had a significant outage in the last 18 months, and each one affected businesses that were not direct customers. Many of the applications you use run on AWS, Google Cloud or Microsoft Azure behind the scenes, so you can be affected by a provider you have never signed a contract with.

Date	Provider	What failed	Effect
12 to 13 November 2026	Microsoft 365	Networking gateway servers overloaded after a latent defect	Email and many Microsoft 365 services unavailable for around a day
25 July 2026	OpenAI	ChatGPT, the API and Codex returned errors	Products built on OpenAI's models failed for their own customers
20 October 2025	AWS	A DNS fault in DynamoDB in the US-EAST-1 region	Disruption to many websites and online services for more than 14 hours
12 June 2025	Google Cloud	An invalid automated update to its API management system	Spotify, Fitbit and Cloudflare were among the services affected

AI platforms deserve particular attention. Many businesses have built AI into customer service, document drafting, coding and data analysis within the last two years, often without a plan for when it is unavailable.

- Record which processes now depend on an AI service, including AI features built into other software you use.
- Make sure staff can still complete those processes manually, and that the knowledge to do so has not been lost.
- Avoid relying on AI for customer-facing processes without a fallback, such as routing enquiries to a person when an AI assistant fails.
- Consider whether an alternative AI provider could be used for critical tasks, and whether your data protection arrangements would allow it.
- Ask your key software suppliers which cloud and AI providers they depend on, and what their own continuity plans are.

Continuity belongs to the business, not IT.

> **Business continuity planning is a business process, owned by the leadership team, and it should decide where technology money is spent.**

An IT outage is often what triggers the plan, so continuity is easily handed to IT as a technical problem. That gets the order wrong.

The business should first decide which functions matter most, who needs to perform them and how long each can be paused. Only then should IT design and cost the technical measures to meet those requirements. Starting with technology tends to produce expensive resilience in some areas and none in others, because nobody asked what the business needed.

© EMH Technology Limited 2026

Core people show why this matters. No amount of IT investment helps if the only person who can run payroll, approve payments or speak to your largest client is unavailable. That risk can only be identified and managed by the business itself.

Lockdown tested only one scenario.

Many organisations believe they already have a continuity plan because everyone worked from home during lockdown. That response worked well, but it tested one scenario: the office was unavailable while people, systems and suppliers kept working. Most other scenarios have not been tested at all.

Scenario	What is lost	Tested by lockdown?
Office inaccessible	Premises	Yes
Cloud or AI platform outage	Email, files, applications or AI tools	No
Loss of internet connectivity	Access to every cloud service from that location	No
Loss of key personnel	Knowledge, authority and relationships held by one person	No
Cyber attack	Systems and data, possibly for weeks	No
Failure of a key supplier	A service or product you cannot easily replace	No

Home working actually makes some of these scenarios harder. Staff now depend on cloud services and their own broadband, and nobody is in the same room to agree a workaround. A plan that only covers the office being closed is a plan for the scenario you have already survived.

Know which systems you depend on.

Start with a list of the systems your business cannot trade without, then decide how long each can be unavailable. This sets your recovery objectives and tells you where to spend money. Typical timeframes to test against are 4, 8, 12, 24 and 48 hours.

System	Typical dependency	Questions to answer
Email	Customer contact, orders, approvals	Could you reach key customers and suppliers by another route within an hour?
Phones and chat	Internal coordination, client support	Does your phone system rely on the same provider as your email?
Files and documents	Contracts, quotes, operating procedures	Can staff reach the documents they need if your cloud storage is unavailable?
Line of business systems	Finance, CRM, case management, stock	Which cloud provider hosts each system, and how do users sign in to it?

© EMH Technology Limited 2026

System	Typical dependency	Questions to answer
AI tools	Drafting, customer service, analysis, coding	Could the work continue manually, and does anyone still know how?
Website and online services	Sales, bookings, donations, customer portals	Which hosting and payment providers would take these offline if they failed?
Security tools	Endpoint protection, device management	Will you be alerted to threats while the admin portals are down?

Practical measures for most organisations include the following.

- Keep an independent communication channel, such as a phone system or messaging tool that does not depend on the same provider as your email, and make sure staff know when to use it.
- Hold an up-to-date contact list for staff, key customers and suppliers somewhere other than your email system, including a printed or offline copy.
- Back up your cloud data, including Microsoft 365 and Google Workspace, with an independent service, because providers' own retention is designed for service resilience rather than your recovery.
- Consider an email continuity service for businesses where a day without email would cause serious financial or reputational harm.
- Store key operating procedures and the continuity plan itself where they can be reached when your main platform is down.
- Understand the sign-in dependencies of your other applications, so that a problem with one identity provider does not take out more than you expect.

Outages are also a favourite moment for criminals. Expect phishing emails and fake “service restored” messages, and remind staff to verify any request to re-enter passwords.

Plan for the people you rely on.

Technology outages are visible, but the loss of a key person is often more damaging and lasts longer. Illness, resignation, holidays or travel can remove the one person who knows how payroll runs or who holds the admin password. Your plan should treat key people as critical in the same way as critical systems.

- Name an owner for continuity in each area of the business, such as support, sales, finance and operations.
- Identify the staff who must be able to work during an incident and confirm they have what they need, including a second way to sign in and be contacted.
- Record who has the authority to invoke the plan, and name a deputy for each of those people.
- Find the tasks only one person knows how to do, and document or cross-train them so that at least two people can carry them out.
- Keep administrative credentials and break-glass accounts secure but accessible to more than one authorised person.
- Agree how staff will be told what is happening and what is expected of them, so that people are not left guessing.

© EMH Technology Limited 2026

Incidents are stressful. Clear roles and simple instructions reduce pressure on staff, and a short debrief afterwards helps the team recover and improve.

Decide in advance how work continues.

A plan is only useful if it tells people what to do differently. For each critical process, write down how it will run when the normal tools are unavailable, and how long that workaround is acceptable.

- Define the trigger for invoking the plan, such as email being unavailable for more than two hours during business hours.
- Prepare short scenario plans for the events most likely to affect you, including a cloud or AI service outage, loss of internet connectivity, power loss, loss of the office and loss of key personnel.
- Set out manual or alternative workarounds for time-sensitive work, such as taking orders by phone, approving payments by a verified call or issuing urgent documents by another secure route.
- Prepare template messages for customers, suppliers and staff, so that you can communicate quickly and consistently.
- Plan how you will return to normal, including checking that delayed messages arrived and reconciling any work done outside the usual systems.
- Record every decision and action during an incident, because this makes the review afterwards far more useful.

Not every outage justifies a full response. Invoking some measures takes time and effort, so your plan should say which actions are worthwhile for an outage of a few hours and which are reserved for longer events.

Test the plan regularly.

The most common failure we see is a plan written once and never used. Systems, suppliers and staff change, and a plan that was accurate two years ago may now point to people who have left or tools you no longer use.

- Run a short tabletop exercise at least once a year, walking through a realistic scenario such as last week's outage.
- Test technical recovery, such as restoring files from backup, rather than assuming it will work.
- Update the plan whenever you add a system, change a supplier or a key person leaves.
- Review the plan after every real incident, including near misses, and record what you changed.
- Write the plan so that anyone in the business could follow it, not only the person who wrote it.

Last week's outage is an ideal starting point for an exercise. Ask your team what happened, what worked and what they wish had been in place.

© EMH Technology Limited 2026

Start with this checklist.

- [ ] Our continuity plan is owned by a named director, not by IT.
- [ ] We have listed our critical systems and agreed how long we can manage without each one.
- [ ] We know which cloud and AI providers our critical systems and key suppliers depend on.
- [ ] We have a way to communicate with staff, customers and suppliers that does not depend on the same provider as our email.
- [ ] Our contact lists and continuity plan can be reached when our main platform is down.
- [ ] Our cloud data is backed up by an independent service, and we have tested a restore.
- [ ] Every process that uses AI can still be completed manually by someone who knows how.
- [ ] We have named who can invoke the plan, and each of them has a deputy.
- [ ] Every critical task can be carried out by at least two people.
- [ ] We have written workarounds and template messages for our most time-sensitive processes.
- [ ] We have tested the plan in the last 12 months and updated it since.

EMH can help you prepare.

EMH Technology has helped businesses and charities plan for disruption for more than 20 years. We can review your current arrangements, identify single points of failure across your technology, people and processes, and help you build and test a practical plan that suits your size and budget. If last week's outage caused problems for your organisation, get in touch and we will help you make sure the next one has less impact.

Sources

1. Microsoft 365 Outage, November 12, 2026: What Went Down and the Timeline (On-Site Technology)
2. Microsoft 365 outage: what went wrong, in plain English (Office Watch)
3. Global outage hits OpenAI's ChatGPT, API and Codex (Unite.AI)
4. Amazon: This week's AWS outage caused by major DNS failure (BleepingComputer)
5. Google Cloud outage analysis: June 12, 2025 (ThousandEyes)

© EMH Technology Limited 2026