protiviti®
Global Business Consulting

Actions Organisations Should Take Now in the Wake of the Latest Major Outages

Six practical steps leaders can complete in the next 72 hours to prepare for disruption

November 19, **2026**

A rash of cascading technology failures over the past week should serve as a wake-up call for leaders to ensure they have clearly defined business continuity measures in place.

In the span of six days:

- 12 November – Microsoft 365 email and collaboration services failed worldwide.
- 13 November – The Federal Aviation Administration issued a nationwide ground stop.
- 16 November – Banking and airline systems experienced disruptions.
- 17 November – The National Security Agency's classified internal network went offline, and Apple reported an outage affecting iCloud and Apple Pay later that day.

Each working day appeared to bring a new wave of outages and disruptions. For organisations, these events raise two immediate questions: Are these events connected, and what should we do now to prepare for the next disruption?

The facts available point to a recurring pattern in the stated causes, not to a single shared cause. Public reporting describes distinct technical causes. At this point, officials and providers have said there is no indication of a cyberattack in any of them.

For leadership teams, the takeaway is not that any single provider or agency is uniquely at risk. Concentration on a small number of platforms, reliance on ageing infrastructure and the pace of change in critical systems have become structural features of how organisations operate, and major outages are now a recurring operating condition rather than a rare event.

What organisations should focus on now

- **There is no evidence these events were cyberattacks, but do not assume the same of your own incidents.** Each organisation still must make that determination quickly, and carefully, using its own evidence.
- **Concentration and legacy infrastructure are both exposure points.** Dependence on a few providers and on ageing systems can each turn a routine event into a major disruption.
- **Change management is a resilience control.** The timing, scope and rollback planning of upgrades and patching on critical systems deserve executive attention, not just IT routine.

Questions leadership teams should be able to answer now

- If a critical provider were unavailable for 24 hours, what would we do, and when did we last test that strategy or plan?
- Who approves maintenance and upgrades on critical systems during business hours, and do we have a rollback plan? If so, what is it?
- How would we decide within hours whether an outage is an attack, and who would we tell first?
- When did we last use or test our backup communications channel with the full decision-making team, and what failed?

Actions to complete in the next 72 hours

None of the following actions requires buying anything. Each can be assigned today and completed within three days, and together they show where an organisation would struggle in the next major outage. The first four are the ones leaders and boards will most want to see owned and dated.

1. **Reaffirm which third parties sit on the critical path.** Note the providers and contractors that inform key processes and flag any that supply more than one critical capability. Ensure the process owners of critical processes are aware of steps to take and the third-party contacts to communicate with in the event of a disruption to services provided.

Why it matters: Every new subscription, integration and contract changes the critical path of critical business services. These blind spots represent real risk.

2. **Test backup communications now.** Confirm that the backup does not share the same identity, network or device dependency as a primary channel, and that current credentials and bridge details are held outside the affected platform. Test at least one manual workaround and record the volume and duration it can support – manual is not the same as sustainable.

   Why it matters: Secondary communications do no good unless they work, and people are aware of them.

3. **Confirm a deputy for every time-sensitive decision.** Do not assume decision makers will be available. Declaring an incident, invoking the continuity plan, approving client and regulatory notifications and authorising emergency spend each need a documented deputy and a clear condition for transferring authority.

   Why it matters: You don't want to decide if a delegate can make decisions 'in the moment'.

4. **Pre-approve customer and employee messages.** Have legal and communications sign off on client notification templates, service desk scripts and FAQs, workforce notices and a holding statement before an adverse event. Workforce notices should tell employees whether to wait, use a workaround or stop work. They should also avoid guessing at a cause and refer questions from the media to communications. Agree on who approves each release and how messages will reach people if normal channels (e.g. email or the intranet) are down.

   Why it matters: Clients and employees start calling within minutes, and anyone without approved language will improvise or escalate. Approvals are slowest in the midst of an incident, so it's best to agree on the wording before one starts.

5. **Keep the crisis toolkit accessible (consider core platforms).** Contact rosters, bridge details, runbooks and the business continuity plan should be accessible, including in offline or printed form, when the systems that normally hold them are not.

   Why it matters: Workarounds succeed only when someone can find the contact list and the plan.

6. **Stay connected and learn from near misses.** Confirm access or active membership in the sector's information sharing forums, such as FS-ISAC, Health-ISAC, CISA alerts or InfraGard, with a named monitor and deputy, and make sure provider status alerts reach that person through a path independent of the primary platform.

   Why it matters: The first question in any outage is whether it is an attack, and peers comparing observations can narrow that gap. A near miss exposes the same gaps as a real incident, at no cost.

Closing thoughts

Provider outages will keep happening, and most will not be the result of attacks. Organisations cannot prevent impact when these systems are unavailable, but they can control how quickly they respond, fail over to alternative methods to resume business and minimise their own customer disruption. The first 72 hours are a practical window to prove that capability while the lessons are fresh and the systems are running.

How Protiviti can help

Protiviti helps organisations prepare for, respond to and recover from adverse events, including technology and third-party outages. Our teams help clients identify their most important business services and the providers behind them. We also test response plans through realistic exercises and build governance (e.g. decision rights, communications and evidence) that holds up on a bad day. When an outage is already underway, we support the response and the recovery that follows.

Protiviti's latest Business & Technology Resilience Guide covers everything from IT disaster recovery and third-party risk to regulations, standards and testing, with practical answers for organisations. View the guide here.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit – enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the Fortune 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 per cent of Fortune 100 and nearly 80 per cent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Contacts

Andrew Retrum
Managing Director
Global Lead, Cyber & Business Resilience
andrew.retrum@protiviti.com

Randy Armknecht
Managing Director
randy.armknecht@protiviti.com

© 2026 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®