Article

May 2026

Is your business ready for the unexpected? Five technology and cyber security priorities for business resilience

Let's be honest, most IT and security leaders know that resilience and continuity planning should be a top priority. But between managing day-to-day operations, keeping the lights on, and responding to the latest threat landscape, it can easily slip down the list.

David Dove
Senior Information Security Consultant
Email david.dove@waterstons.com

When something goes wrong (and at some point, something will) the businesses that recover quickly are the ones that prepared *before* the crisis hit, not during it.

Incidents now trigger full-scale business disruption, not isolated IT outages.

So, whether you're stress-testing your existing plans or starting from scratch, here are five key areas that every business should have firmly on their radar.

1. Cyber incident response: have a plan *before* you need one

When a cyber incident hits, the last thing you want is people scrambling to figure out who does what. A cyber incident response plan, and wider business continuity planning, can be the difference between a contained disruption and a full-blown crisis.

Your plan should clearly define roles, escalation paths, and communication protocols – planning for a loss of systems, not just a quick recovery. And it shouldn't just live with the IT team; operational leaders, legal, HR, comms and the executive team all need to know their part.

Running regular tabletop exercises to pressure-test your plan is a great way to simulate response in a safe, risk-free environment. Mimic a ransomware attack. Walk through a data breach scenario. You'll quickly find the gaps before an attacker does.

It's also worth considering a third-party incident response retainer. Having expert support (psst, like us!) on speed dial means you're not starting from zero when the pressure is on.

2. Backup and disaster recovery: test it or trust nothing

A solid backup and disaster recovery strategy is the foundation everything else is built on. But having backups isn't enough, the question is whether they actually *work* when you need them.

One thing that's often overlooked? Immutable backups. With ransomware attacks increasingly targeting backup infrastructure, having backups that can't be altered or deleted is no longer a 'nice-to-have'. Cloud-based disaster recovery solutions like Azure Site Recovery or AWS Elastic Disaster Recovery can also give you rapid, scalable failover options without the hefty on-premises price tag.

And *please* - test your disaster recovery plan regularly. A backup that hasn't been tested is, frankly, not a backup.

3. Identity and access management: because most breaches start with a credential

Compromised credentials remain one of the most common entry points for attackers, yet many organisations still have gaps in how they manage and control access - particularly around privileged accounts and former employees.

If you haven't already, enforce Multi-Factor Authentication (MFA) everywhere. No exceptions, especially for admin-level access. Pair this with a Zero Trust approach - the principle that no user or device should be trusted by default, regardless of whether they're inside or outside your network.

Privileged Access Management (PAM) tools give you visibility and control over your most sensitive accounts, while applying the principle of least privilege ensures users only have access to what they genuinely need to do their job.

4. Supply chain and third-party risk: your resilience is only as strong as your weakest link

Your own security posture is only part of the picture. The businesses and suppliers you rely on can introduce significant risk into your environment - and that's something many organisations underestimate until it's too late.

Think about the SolarWinds attack - a compromise in a trusted software supplier that cascaded into thousands of organisations worldwide. Supply chain risk is real, and it needs to be actively managed.

Start by conducting thorough third-party risk assessments and building cyber security requirements into your supplier contracts. Validate that your critical suppliers have their own continuity and disaster recovery plans in place. Segment your networks to isolate critical systems, and maintain an up-to-date asset and dependency register so you always know what's connected to what.

Resilience isn't just internal, it's an ecosystem.

5. Continuous monitoring and security awareness: you can't protect what you can't see

The final piece of the puzzle is visibility, both technical and human. Even the best tools in the world won't protect you if your team doesn't know how to spot a phishing email, and even the most security-aware workforce can't compensate for a lack of threat detection capability.

On the technical side, a SIEM solution and/or a Security Operations Centre (SOC) gives you 24/7 monitoring and the ability to detect and respond to threats in real time. Endpoint Detection & Response (EDR) tools add another layer, helping to contain threats quickly at the device level. Regular vulnerability scanning and penetration testing rounds this out by proactively identifying weaknesses before attackers can exploit them.

On the human side, invest in ongoing security awareness training for all staff — not just a once-a-year tick-box exercise, but regular, engaging content that keeps people sharp. Phishing simulations are a great way to keep awareness high and identify where additional support is needed.

Where do you start?

The good news is that you don't need to tackle all of this at once. Many organisations already have some of these elements in place, but the challenge is often around the processes, governance, and testing rigour needed to make them truly effective.

A maturity assessment across these five areas is a great way to understand where you are today, identify the gaps, and build a prioritised roadmap that's realistic for your business.

Leaders need to stop asking “Could we survive a cyber attack?”, and start planning how long their business can operate effectively while key systems are unavailable.

We can help you work it out. Get in touch at info@waterstons.com.au