littlefish CYBER SERVICES GROUP | SECURITY INSIGHTS

BACKUP, RECOVERY, AND RESILIENCE

A practical guide to staying in control when things go wrong.

CYBER SERVICES

When systems fail, what happens next?

Most organisations invest heavily in stopping cyber incidents from happening – and rightly so. Prevention, detection, and response are essential.

But here's what experience shows time and again. When disruption hits, it's not the organisations with the longest tool lists that recover best. It's the ones that have put real thought into recovery, continuity, and how decisions get made when pressure is highest.

Moreover, the FCA has been refocusing hard on operational resilience, warning that outages, supplier failures, and cyber incidents aren't abstract risks – they're routine tests of whether organisations can remain within their impact tolerances and keep critical services running. Regulators have made one thing clear: resilience isn't optional, and hoping a supplier or cloud platform won't fall over isn't a strategy.

Backup, recovery, and resilience aren't about planning for failure. They're about staying calm, staying in control, and giving teams the confidence to act when systems are unavailable and the clock is ticking.

This guide draws on practical experience across cyber, backup, and resilience, focusing on what actually helps organisations regain control and move forward.

Warm regards,

Sean Tickle,
Cyber Services Director

> ***Backup, recovery, and resilience aren't about planning for failure. They're about staying calm, staying in control and giving teams confidence to act when systems are unavailable.***

CYBER SERVICES

Why backup still matters

Cyber security has changed dramatically over the last decade. Organisations are more aware of risk, more regulated, and better defended than ever before. Detection and response platforms, SIEM, and continuous monitoring all play a vital role in spotting threats early and limiting damage.

And yet, incidents still happen.

According to the UK Government's Cyber Security Breaches Survey 2025, 43% of UK businesses experienced a cyber security breach or attack in the past 12 months. For medium and large organisations, the picture is even starker – 67% of medium businesses and 74% of large businesses reported an incident.

The reality is that strong cyber security reduces risk, but it does not remove it entirely. No organisation, regardless of size or maturity, is immune. When an incident does occur, the ability to recover becomes just as important as the ability to defend.

That is where backup plays a foundational role. Backup is the safety net that allows data to be restored, services to resume, and operations to stabilise. Without it, even a relatively contained incident can escalate quickly – turning disruption into a prolonged business crisis that affects far more than IT.

The true impact of poor recovery planning

The consequences of a serious cyber incident rarely stop at IT.

Operational disruption quickly spills into customer experience, revenue, productivity, and internal confidence. In regulated sectors, the stakes are even higher – outages can trigger compliance concerns, reporting obligations, and close scrutiny from regulators or commissioners. And while systems may come back online, reputational damage has a habit of sticking around far longer.

There's a reason this matters. Research consistently shows that organisations with clear incident response and recovery plans significantly reduce the overall cost of a breach. Faster recovery means less downtime, lower financial impact, and a far better chance of maintaining trust with customers, partners, and stakeholders.

The opposite is also true. Organisations without reliable backups often find themselves rebuilding from the ground up. Systems need to be reconstructed, data pieced back together where possible, and manual workarounds put in place just to keep things moving. What could have been a controlled recovery stretches into weeks or months, amplifying both operational strain and reputational harm.

This is why backup is not a technical afterthought or a boxticking exercise but a core component of business resilience – one that quietly determines how well an organisation copes when pressure is highest.

> ***Research consistently shows that organisations with clear incident response and recovery plans significantly reduce the overall cost of a breach.***

CYBER SERVICES

Unseen, until it really matters

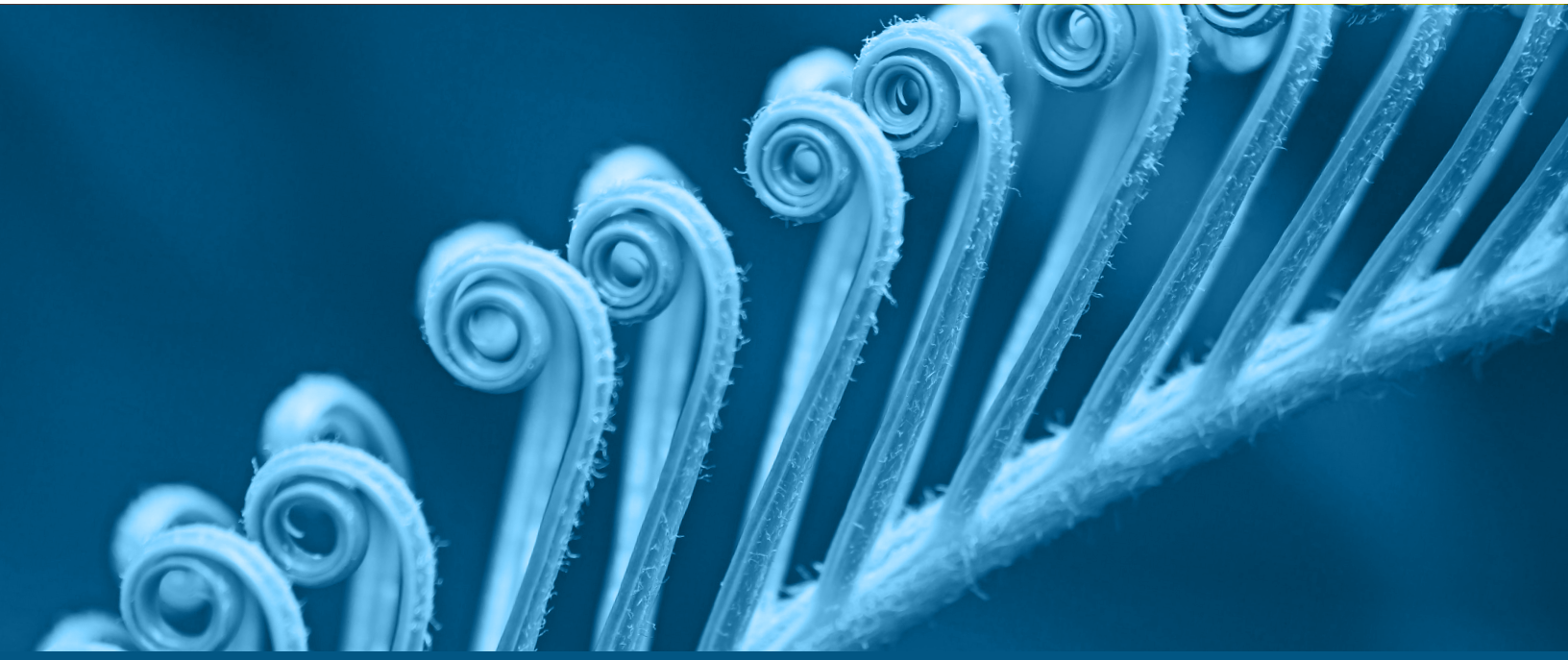
Backup serves a far bigger purpose than simply restoring files.

From a compliance perspective, it underpins a wide range of regulatory obligations – from GDPR and PCI DSS to sector-specific frameworks that expect organisations to demonstrate control, recoverability, and good governance. Increasingly, it is also a baseline requirement for cyber insurance, where insurers look for clear evidence that recovery is realistic, not theoretical.

Operationally, the value is even clearer. Effective backup removes uncertainty at exactly the moment leaders can least afford it. When recovery time and recovery point objectives are understood and achievable, decision-making becomes calmer, faster, and more confident. The focus shifts from firefighting to managing impact.

The difference this makes is well documented. Organisations with mature backup strategies are far more likely to restore data within hours or days, allowing critical services to resume quickly and disruption to be contained. Those without reliable backups often face recovery timelines measured in weeks or months, with financial consequences that escalate rapidly. In the most extreme cases, prolonged data loss has been linked to organisations failing altogether within a year of an incident.

Remember, backup does not eliminate risk, but it dramatically reduces the fallout when something goes wrong. Quietly, consistently, it does the heavy lifting that keeps disruption from turning into crisis.



CYBER SERVICES

Why backup still gets overlooked

Despite clear evidence of its value, backup maturity remains uneven across organisations. Not because people don't care – but because it's often misunderstood, underestimated, or quietly deprioritised.

Awareness is a big part of this. Many organisations underestimate the likelihood or impact of data loss, particularly if they've been fortunate enough to avoid a major incident so far. Others assume that existing controls, or a move to the cloud, automatically mean they're covered.

Cost is another perceived barrier. Backup is sometimes seen as expensive or overly complex, especially as data volumes grow. In practice, the economics rarely stack up that way. The cost of recovery failure – prolonged downtime, operational disruption, reputational damage – almost always outweighs the cost of getting backup right in the first place.

Complexity plays its part too. Managing backup environments, schedules, retention policies, and testing takes time and expertise that many internal teams are already stretched to provide. Without clear ownership and governance, backup processes can drift, becoming inconsistent, outdated, or quietly unreliable.

One of the most persistent misconceptions relates to cloud services. Moving to platforms such as Microsoft 365 is often assumed to mean data is fully backed up by default. In reality, cloud providers operate under a shared responsibility model. While the platform itself is resilient, responsibility for data protection and recovery still sits firmly with the customer.

In other words, backup rarely fails because it's unimportant. It fails because assumptions go unchallenged – until an incident forces the issue, that is.

CYBER SERVICES

From backup to resilience

One of the most important shifts recently is the move away from viewing backup in isolation.

Traditional recovery planning often focused solely on restoring data and systems after an incident. Modern resilience strategies recognise that recovery is also about people, communication, and coordination during disruption.

When core systems are unavailable, teams still need to communicate securely, share information, and make decisions. Without a safe environment to do this, even organisations with strong backups can struggle in the critical early hours of an incident.

This has led to a broader approach to resilience, one that pairs backup and recovery with secure fallback environments that keep the business moving even when primary systems go down. These environments run independently of your core estate, reducing the risk of further compromise, minimising disruption to wider operations, and giving teams a clean space to regain control. Better still, they can be brought online quickly, often within an hour, so leadership has the clarity and stability needed to steer the response effectively.

Resilience, in this context, is about maintaining momentum. It allows organisations to stabilise operations, protect trust, and manage response

CYBER SERVICES

Changing the recovery mindset

One of the most important shifts in recent years has been moving away from viewing backup as a standalone technical function.

Traditional recovery planning focused almost entirely on restoring data and systems after an incident. Modern resilience strategies take a broader, more realistic view. Recovery isn't just about technology, it's about people, communication, and coordination while disruption is still unfolding.

When core systems are unavailable, work doesn't pause. Teams still need to communicate securely, share accurate information, and make decisions under pressure. Without a safe environment to do that, even organisations with strong backups can struggle in the critical early hours of an incident (when clarity matters most!).

This has driven a more holistic approach to resilience. Backup and recovery are now increasingly combined with secure fallback environments that allow organisations to continue operating during disruption. Designed to sit independently from primary systems, these environments reduce the risk of further compromise and give leadership teams a trusted space to regain control quickly.

In this context, resilience is about maintaining momentum. It helps organisations stabilise operations, protect trust, and manage response activities with confidence while recovery work is underway.

> ***Resilience is not just about restoring systems. It's about giving people the ability to lead, communicate, and make decisions while disruption is still unfolding.***

CYBER SERVICES

Resilience done properly

Organisations with mature backup and resilience strategies tend to share a few tell-tale traits – and none of them are accidental.

They're clear on what really matters

Recovery objectives are aligned to business priorities, not just technical metrics. Critical systems and data are well understood, recovery timelines are agreed, and there's no scrambling for answers when pressure is on.

They take fragility out of the equation

Backup processes are automated wherever possible, reducing reliance on manual intervention and lowering the risk of human error at exactly the wrong moment. Backups are protected, isolated, and secured, so the safety net doesn't become another point of failure.

They test regularly

Regular testing turns assumptions into evidence, exposes gaps early, and builds confidence across both technical teams and leadership.

More advanced organisations plan to operate during disruption, not just recover afterwards. Secure fallback environments keep communication and decision-making moving, helping teams stay in control when systems are offline.

Sean Tickle,
Cyber Services Director

"Research consistently shows that organisations with clear incident response and recovery plans significantly reduce the overall cost of a breach.

CYBER SERVICES

Going beyond *"we think we're covered"*

Every organisation's environment is different, but the questions that reveal whether a backup strategy will hold up under pressure are surprisingly consistent.

Leaders should be clear on how quickly data can be recovered after an incident, and how much data loss is genuinely acceptable. Recovery time and recovery point objectives need to be defined, documented, and tested – not guessed at when systems are already offline.

It's also important to understand what backups are in place, how often they run, and whether anyone is actively checking that they complete successfully. Backups that aren't monitored or tested can create a dangerous sense of reassurance without delivering real protection.

Security matters here too. Access to backup data should be tightly controlled, authentication strengthened, and backup environments monitored for unauthorised activity. After all, a backup that can be compromised is not much of a safety net.

Answering these questions provides a realistic view of current capability, and a clear starting point for strengthening resilience.

The fundamentals that make recovery work

Several well-established principles continue to underpin effective backup strategies.

The 321 rule remains a useful starting point, ensuring multiple copies of data exist across different storage types, with at least one copy held offsite. Automation reduces reliance on manual processes and improves consistency.

Encryption protects backup data from unauthorised access, while version control allows organisations to recover from corruption or accidental deletion. Offsite and cloud storage provide resilience against physical incidents such as fire or flood.

Importantly, backup should be integrated into a wider disaster recovery plan that defines roles, responsibilities, communication paths, and escalation procedures. Backup alone does not create resilience; it supports it.

CYBER SERVICES

Ready for reality?

Ultimately, backup and resilience are about confidence. Confidence that data can be restored, that teams can communicate securely, and that leaders can make clear decisions when pressure is highest.

When those foundations are in place, incidents stop feeling overwhelming. Recovery becomes structured rather than reactive, and organisations protect outcomes, not just infrastructure.

Backup isn't about expecting the worst. It's about being ready for reality.

As digital estates grow more complex and scrutiny increases, hoping disruption won't happen cannot be your organisation's strategy. Being able to recover quickly and calmly should be.

littlefish
CYBER SERVICES GROUP

If this has prompted questions about your own backup or resilience approach, please feel free to get in touch – **a conversation now can make a real difference later.**

Microsoft Solutions Partner – Modern Work – Specialist – Adoption and Change Management
Microsoft Solutions Partner – Data & AI Azure – Specialist – AI Platform on Microsoft Azure
Microsoft Solutions Partner – Business Applications – Specialist – Low Code Application Development
Microsoft Solutions Partner – Security – Specialist – Cloud Security
Microsoft Solutions Partner – Modern Work – Specialist – Modernize Endpoints
Microsoft Solutions Partner – Security – Specialist – Threat Protection

aws
CREST SOC
CYBER ESSENTIALS
ISO 9001 ISOQAR REGISTERED
ISO 14001 ISOQAR REGISTERED
ISO 27001 ISOQAR REGISTERED

Get in touch today
0330 390 2002
info@littlefish.co.uk
littlefish.co.uk