



SMS WHITE PAPER

SECURITY & BACKUP

ENCRYPTED, EXPOSED, OFFLINE: WHY SECURE BACKUP IS NOW A BOARD-LEVEL PRIORITY

This white paper explores why secure backup, cyber protection and clean recovery are essential for modern organisations. It explains how SMS helps businesses strengthen their defences, protect Microsoft 365 data, reduce downtime and recover confidently with managed security and backup solutions including Acronis Cyber Protect.

smsbusinesscloud.com



The moment no business wants to face

It usually starts as a normal working day. A member of staff clicks a link that looks legitimate. A supplier invoice opens. A familiar password is reused. A remote access tool is left exposed. A patch has been missed. Nothing feels urgent, and nothing appears broken. Then, gradually, files begin to disappear.

Shared folders stop opening. Finance cannot access invoices. Customer service systems fail to load. Directors cannot open board packs. Staff reboot their machines, hoping it is a temporary glitch, only to be met with the same message again and again: Your files have been encrypted.

At that point, the issue is no longer a technical inconvenience. It is an operational crisis. Work stops. Decisions carry weight. The business is forced to answer questions it may never have fully considered before. Who can still work? Which systems are safe to touch? Are backups clean, or have they been compromised too? Has data been stolen? Can payroll still run? Can customers still be supported? Should systems be restored, rebuilt, isolated, or left offline? And ultimately, who makes that call under pressure?

Organisations that recover quickly and confidently are rarely the ones making those decisions for the first time during an attack. They are the ones that had already defined what “good recovery” looked like, long before ransomware tested them.

Backup Is Not the Same as Recovery

Many organisations assume they are protected because they have a backup. That confidence can be risky if recovery has never been tested.

Effective backup means knowing what is protected, how often it is backed up, how quickly it can be restored, and whether the backup itself is safe from ransomware. The NCSC recommends regular backups, tested recovery procedures, and secure offline or cloud storage, as attackers increasingly target backups to remove recovery options. It also advises checking that backups are malware-free before restoration.

True resilience needs more than data copies. It requires secure backup, threat detection, malware scanning, patching, monitoring and expert recovery support working together.

The Facts

in 2025

43%

OF UK BUSINESSES REPORTED EXPERIENCING A CYBER SECURITY

An increase of

70%

OF RANSOMWARE VICTIMS IN 2025

According to Sophos, it costs an average of

\$1.5 MILLION

FOR RANSOMWARE RECOVERY

What would you do if everything was encrypted?

Every organisation should walk through this scenario before criminals force them to do so. Imagine that by 8:30 tomorrow morning your file shares are encrypted, several laptops are unusable, your finance system is offline and staff cannot access shared documents. Your Microsoft 365 data may be affected. Your last backup may contain malware. Customers are already asking questions, and pressure is mounting to pay.

Responding effectively requires more than panic, goodwill and a handful of old backups. It requires a structured recovery approach. Affected systems must be contained to stop the spread. Clean recovery points must be identified. Entry points such as phishing, exposed remote access, missing patches or stolen credentials must be understood. Systems must be restored in priority order, and recovery must be performed cleanly without reintroducing malware. Finally, controls must be strengthened to prevent the same attack from succeeding again, while communication with staff, customers and stakeholders remains clear and controlled.

Businesses that survive ransomware with minimal disruption are the ones that have already embedded this process into their security and backup strategy.

The SMS approach: complete protection, no compromise

- SMS provides managed protection across the full IT environment, combining backup, cyber security and compliance into one clear service.
- With 24/7 UK-based expert support, businesses have access to experienced specialists when protection, recovery or guidance is needed most.
- Through Acronis Cyber Protect, SMS brings secure backup and cyber defence together to help create real cyber resilience.
- AI-powered threat detection and ransomware protection help identify attacks early and stop files being encrypted.
- Automated backup, cloud storage and disaster recovery help restore systems quickly after cyber incidents, crashes or hardware failure.



Choosing the right level of protection

SMS offers scalable Acronis Cyber Protect plans, from core backup to complete cyber defence. Essentials covers file and image backup, cloud storage, anti-malware, ransomware protection and simple management. Standard adds advanced backup, hybrid storage, patch management and malware-scanned recovery for more complex environments. Advanced provides full cyber protection, continuous data protection, vulnerability assessments, access control and audit logging for high-risk organisations.

Beyond backup: protecting the wider attack surface

Ransomware often starts quietly, with attackers gaining access and moving through systems before encryption begins. SMS reduces this risk with layered protection across email security, email archiving, Microsoft Cloud Application Security and Azure Information Protection.

Together, these services help block threats, support continuity, improve data visibility and protect sensitive Microsoft 365 information. Security works best when every layer supports the next: prevention, protection, monitoring and recovery.

Why managed protection matters

Cyber security tools only protect a business when they are properly configured, monitored, updated and tested.

Many organisations lack the time or expertise to manage multiple platforms effectively. Sophos found that 63% of ransomware victims cited a lack of people or skills as a contributing factor. SMS closes that gap with 24/7 UK-based support and over 15 years of Acronis Cyber Protect experience, ensuring the right protection is in place and ready when needed.



The business case for acting now

Organisations often delay cyber resilience until something goes wrong, but by then it may be too late. Like insurance or business continuity planning, its value is proven during a crisis. Strong resilience reduces downtime, data loss, ransom pressure, compliance risk and recovery cost, while the NCSC confirms that regular, secure backups are one of the most effective ways to recover from ransomware.

Build ransomware resilience before you need it

If you want to reduce ransomware risk and be confident you can recover cleanly when it matters, explore the full SMS [Security & Backup range](#) to see how we protect data, systems and Microsoft 365 end to end. For organisations ready to take a more integrated approach, Acronis Cyber Protect from SMS combines secure backup and cyber protection into a single, resilient platform designed for real-world recovery. If you already know what level of protection you need, you can also buy online through the SMS portal and put that protection in place quickly and simply.

WHY SMS

Who We Are

We are a UK-based managed cloud solutions provider, helping organisations adopt and manage Microsoft 365, Azure and modern workplace tools with confidence. Since 2006, we have supported over 4,500 customers with 24/7/365 UK support, backed by Microsoft Modern Work Partner status and Cyber essential certified.

Our Mission

Our mission is to remove the technical burden and make cloud services simple. From helping customers choose the right solution to setup, support and everyday use, we deliver a hassle-free experience backed by fantastic customer service. We focus on giving businesses confidence to work securely.

What We Do

We make it easy to build, migrate and manage cloud solutions, so businesses can focus on what matters. From Microsoft 365 and productivity to security, backup, infrastructure and communications, we bring reliable cloud services together under one roof with end-to-end UK-based support.

Our Vision

Our vision is to make cloud technology simple, secure and genuinely useful for every business. We aim to be the trusted cloud partner that keeps organisations productive, protected and supported through reliable services, expert guidance and 24/7/365 UK support.

Speak to us today and take the next step towards stronger cyber resilience.

Do not wait until ransomware, data loss or downtime forces the conversation. SMS can help you review your current protection, identify gaps and build a secure backup and recovery strategy that works when it matters most.

Let's Talk →