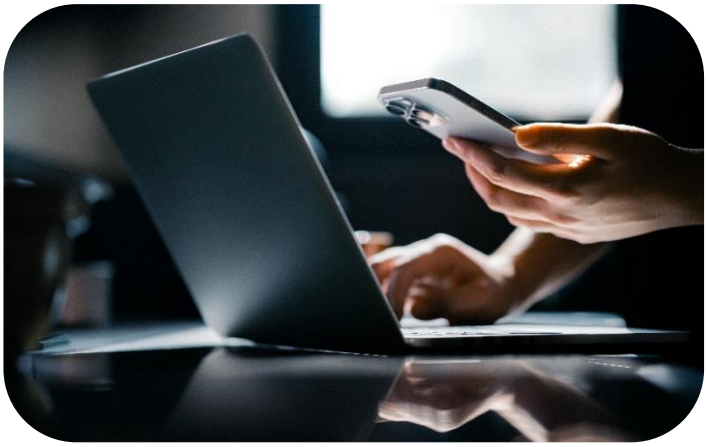
Cyber – Back-ups

This Loss Prevention Standard discusses the importance of data back-ups in helping to avoid cybersecurity related interruption.

Version: 1.0
Date: 23rd July 2026

Cyber – Back-ups

Introduction



Back-ups are a fundamental cyber resilience control and provide businesses and organisations with primary means of recovering from cyber incidents like ransomware, accidental deletion, insider threats, and operational failures.

Effective back-up arrangements help protect the availability, integrity, and recoverability of business-critical data and systems.

The National Cyber Security Centre (NCSC) identifies regular back-ups as one of the most effective methods for recovering from ransomware and other destructive cyber incidents.

The Importance of Back-ups

Organisations, no matter the size, are increasingly at risk from a range of risk categories, including but not limited to:

- Ransomware, including cyber crime
- Insider threats
- Human error
- System failures
- Cloud service outages
- Supply chain incidents

There is clear evidence of threat actors conducting reconnaissance to locate, encrypt, delete or corrupt back-ups before launching their ransomware attack to increase pressure on organisations to pay the ransom. Ensuring a robust back-up procedure is in place underpins an organisation's ability to respond and recover more effectively.

The General Principles of Back-ups

Before arranging a formalised data back-up and recovery strategy, organisations need to identify their critical assets.

Some examples of generalised critical assets can include, but are not limited to:

- Critical business services e.g., payroll and human resources.
- Key business applications.
- Sensitive information assets.
- Infrastructure systems.
- Cloud-hosted systems.

These critical assets then need to be prioritised based on business impact and the recovery strategy. Some key questions to consider for prioritisation are:

- What systems are essential to operations?
- What data cannot be recreated?
- How long can the organisation tolerate an outage?
- What recovery point objective (RPO) is acceptable?
- What recovery time objective (RTO) is acceptable?

Without a robust back-up and recovery plan, organisations face an increased risk of permanent data loss, extended downtime, and regulatory non-compliance, all of which can severely impact operations and reputation.

Key Things to Remember

1. It is a common misconception that cloud file synchronisation and collaboration platforms like Google Drive or OneDrive are a back-up, that is not the case. Adopting cloud infrastructure does not replace the requirement to back up data and systems.
2. Organisations should understand their cloud provider responsibilities, alongside protecting admin accounts and applying multi-factor authentication (MFA) to all privileged users.
3. Keep an offline laptop or other device, containing a copy of your insurance policy, Cyber Incident Response Plan, Business Continuity Plan and any other relevant crisis management documents.
4. Back-ups are critical and should be considered as a business as usual (BAU) activity, alongside other key cyber preparedness activities.
5. Ensuring back-ups are ransomware resistant is key. Some core principles include segregating networks, air gapping (using a computer, network or system that is physically isolated from unsecured networks) and separating credentials for admin accounts and monitoring.

Critical Steps

ARMS Cyber would recommend that all organisations, where possible, implement the measures below. This is in line with NCSC guidance and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

Data Back-up Policy

Organisations should develop and document a data back-up policy that defines the scope, frequency, and retention periods of back-ups, aligned with business and compliance requirements. The policy should cover all critical systems and data types, and include provisions for legal, regulatory, and operational needs.

The governance surrounding this data back-up policy is also fundamental to ensuring effective oversight and enhanced cyber resilience. There needs to be a clear owner (or owners) of the data back-up policy, with a standing agenda item at associated governance meetings to ensure effective oversight. These owners should have role-based access control, with additional security measures such as MFA, privileged access management and separation of duties.

3-2-1 Back-up Strategy

Organisations should implement the 3-2-1 back-up strategy: maintain three copies of data, on two different media types, with one copy stored offsite or in a secure cloud environment.

This approach enhances resilience against data loss due to hardware failure, cyber incidents, or physical disasters. For example:

System Copy	Location
Payroll	Live environment
Payroll 2	Secure back-up platform
Payroll 3	Offline or immutable storage

There is anecdotal evidence of threat actors conducting reconnaissance once they have gained a foothold in an organisation's network to seek information on cyber insurance coverage, and the associated cover for ransomware.

Important: Aviva strongly recommends that:

- Organisations retain their cyber insurance policy in a safe, offline environment, whether that is a standalone, offline or air-gapped computer.
- Other critical documentation be stored in the same location, such as your cyber incident response plan, business continuity plan and other relevant crisis management documentation.

Back-up Security Controls

Organisations should be protecting back-ups with encryption and access controls to prevent unauthorised access or tampering. This includes using strong encryption standards, restricting access to back-up repositories, and monitoring for suspicious activity.

Advanced Encryption Standard (AES) 256-bit encryption is widely implemented and is the standard recommended by ARMS Cyber for organisations seeking strong data protection.

Immutable Back-up Protection

Organisations should implement immutable back-up solutions. This ensures that backed up data cannot be altered, deleted, or encrypted by malicious actors. This includes using write-once-read-many (WORM) storage or cloud-based immutability features to safeguard against ransomware and insider threats, ensuring reliable recovery in worst-case scenarios.

Back-up Testing Procedures

Organisations should be regularly testing back-up and recovery procedures. Without testing back-up procedures, it is impossible to know the associated timeline for restoring systems and data from back-ups. This should include full restoration tests, to verify data integrity and ensure timely recovery. Testing should be documented and include validation of RTOs and RPOs. It will also provide assurance on staff competency and ensure those who are responsible for decision making are practiced in their roles.

Suggested testing timeframe below:

Test Type	Frequency
File restoration	Monthly
Application recovery	Quarterly
Full system recovery	Annually
Disaster recovery exercise	Annually

Staff Training on Back-up Procedures

Organisations should offer training to relevant personnel on back-up and recovery procedures, highlighting their role in disaster recovery and data protection. This can be done through Tabletop Exercises (TTX) and include escalation protocols and guidance on responding to data loss scenarios.

Back-up System Maintenance

Organisations should keep back-up systems and software up to date to address vulnerabilities and maintain compatibility with current infrastructure. This includes applying patches, upgrading versions, and validating integration with evolving IT environments.

Contact Information

United Kingdom

Please visit Aviva Risk Management Solutions or email us at riskadvice@aviva.com. To speak to one of our advisors, call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Canada

Please visit Aviva Risk Management Solutions | Aviva Canada or email us at arms.canada@aviva.com

Ireland

Please visit Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland or Email us at armsireland@aviva.com

Specialist Partner Services

Aviva have created a network of Specialist Partners to complement our in-house capabilities and to enable our policyholders to benefit from a wide range of risk management solutions at preferential rates and terms. Together, we provide solutions to help with the significant challenges of modern-day risk management.

Note: These partner relationships are wholly for the benefit of our policyholders with no income to Aviva.

The following Specialist Partners provide products or services in relation to risk guidance provided, discussed or referenced in this Loss Prevention Standard.

United Kingdom

- Cyber security services - **CSA Cyber**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Ireland

For more information please visit: Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland

Canada

For more information please visit: Our Specialist Partner Network | Aviva Canada

Standards, Sources and Useful Links

Canada

- Canadian Centre for Cyber Security

United Kingdom

- NCSC – Cyber Essentials
- National Cyber Security Centre (NCSC)

Other

- The European Union Agency for Cybersecurity (ENISA)

Additional Information

Loss Prevention Standards

These documents set out best practice recommendations to help reduce the likelihood and impact of losses.

Relevant Aviva Loss Prevention Standards include:

- **Cyber - Respond and Recover.**
- **Cyber - Supply Chain Risk Management**
- **Cyber - Ransomware**
- **Cyber - Respond and Recover**
- **Cyber - Incident Response Process**
- **Cyber - Homeworking Security**
- **Cyber - 12 Top Tips to Protect Against Cyber Attacks**
- **Cyber - Security Certifications for Organisations**
- **Cyber - Security Testing**

Please visit Loss Prevention Standards to view the full library.

Aviva Risks Training Solutions (United Kingdom Only)

Aviva Risk Training Solutions, delivered through our Specialist Partner, SafetyCulture, provide free, bite-sized learning modules exclusively for Aviva policyholders.

Relevant courses include:

- **Cyber Fundamentals**
- **Social Engineering**

Please visit Aviva Risk Training Solutions for further guidance.

23rd July 2026

Version 1.0

ARMSGI4452026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.