http://doi.org/10.7207/twgn26-03

Cyber Security and Resilience for Digital Preservation

Part 3: Respond

Heather Lowrie and Garth Stewart

DPC Technology Watch Guidance Note

July 2026

DigitalPreservationCoalition

ISSN: 2048-7916

This report is published by the Digital Preservation Coalition (DPC). The DPC is an international charitable foundation which supports digital preservation and helps its members around the world to deliver resilient long-term access to digital content and services. In addition to the publication of reports on a range of themes which cover the state of the art in digital preservation, the DPC also supports its members through community engagement, targeted advocacy work, training and workforce development, identification of good practice and standards, and through good management and governance. Its vision is a secure digital legacy.

Discover the DPC's publications, including the latest updates and revisions, at:
https://www.dpconline.org/digipres/discover-good-practice/tech-watch-reports

Find out more about the DPC, the support it offers and how to become a member at:
https://www.dpconline.org/about/join-us

DPC Cyber Security and Resilience Guidance Note Series

Organizations that carry out digital preservation activities operate in an increasingly hostile cyber environment. Threats have grown in frequency, scale, and sophistication, placing unique and irreplaceable collections at risk. Sadly, it is now a case of - *not if, but when* - any organisation holding digital collections of long-term value is subject to cybercrime.

This creates pressure on digital preservation practitioners to understand this issue to a reasonable level of detail and identify key cyber threats to their collections. It is rare that practitioners will be able to confront these threats alone: collaboration and engagement with other teams such as IT will be a likely key next step. This collaboration should lead to the application of appropriate cyber security measures that protect digital collections as far as possible and enable response to a cyber-attack.

However, cyber security is a challenging, often overwhelming subject, especially for practitioners who may have limited time and resources, yet need to understand the following areas:

1. Where to begin with a subject like this: what are the risks?
2. What successful effective pathways towards engagement look like.
3. How to put plans into action so that attacks can be neutralised, impacts can be mitigated, and recovery is possible.

The DPC has published a set of three Guidance Notes to support practitioners in this effort. They will support practitioners and organizational leaders in developing effective responses while maintaining business continuity and safeguarding staff wellbeing. They also encourage organizations to embed cyber security within digital preservation governance and operational practice in ways that protect collections while enabling usability, access, and long-term resilience.

The earlier Guidance Notes in this series outlined an approach to understanding the cyber threats facing digital preservation and effective stakeholder engagement to address them. In this final Guidance Note, we provide practical recommendations for managing risks associated with common digital preservation activities, alongside a roadmap template to support next steps. Technical terminology used throughout this document is defined within the Glossary.

1 Practically embedding security

In this Guidance Note series we have seen how digital preservation and cyber security, when collaboratively delivered, can complement and strengthen one another. Nevertheless, digital preservation activities can and do introduce cyber risks: requiring practitioners to work with high-risk materials and navigate scenarios with uncertain outcomes. Practically embedding good cyber security practice into these activities is key: this section provides guidance on doing so against a selection of typical digital preservation activities and requirements.

1.1 Access to Removable Media

Content transferred to digital preservation organizations is often historical (for example, five or more years old) and/or large scale (ranging from gigabytes to petabyte scale). As historical data carriers, removable media such as USB drives, external hard drives, camera cards, and optical discs will continue to play an important role in the ingest of digital collections. Recommended controls for working securely with removable media include:

- Using **dedicated, isolated ingest workstations** that are separate from corporate networks where appropriate.
- Applying **automated malware scanning** to all media before use.
- Mounting devices in **read-only mode** wherever technically feasible to reduce the risk of unintended modification or execution of malicious content.
- Maintaining **comprehensive logging and audit trails** for all media access events.
- **Restricting access** with role-based permissions to authorized staff only.

1.2 High-Risk and Unusual File Formats

Preservation workflows frequently encounter obsolete or high-risk file types, including disk images, executable content, embedded scripts, and legacy formats. To handle these safely:

- Use '**sandboxed' or virtualized test environments** to contain potential threats when examining or processing high-risk content.
- Maintain **documented handling procedures** for problematic file types and formats.
- Develop and regularly update **file format risk registers** to track known vulnerabilities, dependencies, and specialist processing requirements.
- **Separate** rendering, viewing, and analysis environments from primary preservation storage to minimise the risk of malware or other threats reaching preservation systems.
- The DigiPres Workbench provides links to tools for analysing and understanding unusual file formats in more detail (Jackson, 2026a).

1.3 Unknown or Unprocessed Collections

Collecting organizations frequently receive "collections in the wild," such as unsorted hard drives, legacy servers, or private archives. Often, the collecting organization may be the last point of preservation for the collections of insolvent enterprises, mothballed industries, or deceased individuals, where information about potential security risks may be limited or unavailable. These materials often arrive with incomplete or uncertain provenance and assurance, increasing the risks of malware, sensitive data exposure, and data corruption.

Recommended handling strategies include:

- **Quarantined storage zones for initial ingest and assessment**. Establish dedicated environments for initial ingest and assessment before material enters preservation systems.
- Automated threat scanning. Use **multiple anti-virus engines or threat detection tools** where feasible. Diversity in the types of scanning tools used, and their placement within the digital preservation workflow (for example during ingest, preservation processing, or other stages) can increase the likelihood that threats are identified and assessed promptly.
- Implement **structured assessment processes and triage workflows** before material enters the main repository. Where necessary, **digital forensics tools** can be used to unpack or decompress complex digital objects, enabling more complete file characterisation and malware assessment.
- Maintain **strict segregation** between pre-processed acquisitions and processed or 'ingested' collections.
- Document a **clear chain of custody** for all transfer, handling, and processing steps. Recognised metadata standards such as PREMIS may be useful in recording information as part of documentation workflows (PREMIS, 2026).

1.4 Space for Innovation

As noted in previous publications in this Guidance Note series, digital preservation is an evolving field that must adapt alongside technological change. It requires experimentation with new tools, formats, and approaches. Practitioners should work with their organizations to support trustworthy innovation by:

- Providing **isolated research and development (sandbox) environments** separate from production systems. Ensure experimental activities are conducted separately from production systems to reduce operational risk.
- **Maintain** test repositories. Use dedicated test environments for evaluating experimental workflows.
- **Conduct proportionate risk assessments**. Evaluate potential technical, operational, legal, and security risks associated with new approaches.
- Define clear **pathways for implementation**. Establish processes for moving successful experiments into production environments, ensuring innovations are introduced safely and sustainably.

1.5 Using Open-Source

Open-source tools are central to digital preservation practice, enabling practitioners to develop scripts and methods to overcome common challenges, and share solutions for broader community benefit. The COPTR website is a valuable resource for identifying digital preservation tools and approaches (COPTR, n.d.).

When selecting open-source tools for use within preservation infrastructures, organizations should consider:

- **Who** created the tool and who currently maintains and supports it?

- Is the **source code** for the tool publicly available, actively maintained, and regularly reviewed and updated?
- How widely is the tool **adopted and supported** by the digital preservation community?
- Is the tool **regularly updated and patched** to address security vulnerabilities?
- Is there any form of **certification**, attestation, independent review, or community assurance supporting its safe use?

Close collaboration with IT and cybersecurity colleagues is essential to enable appropriate due diligence, risk assessment, and impact analysis before introducing any tool into production environments. Free platforms for experimenting with open-source tools in isolated environments are available and may support assessment and evaluation (OPF, 2026; Jackson, 2026b).

1.6 Supply Chain Security

Effective supply chain security requires a combination of technical, organizational, and contractual controls. Procurement and contract management processes for services that support digital preservation, including storage, applications, and compute infrastructure, can be complex. The following recommendations may assist practitioners when collaborating with procurement, IT, security, and other relevant teams within their organizations:

- **Vendor and community due diligence**: Evaluate the stability, governance, security practices, and long-term sustainability of commercial vendors and open-source communities before adoption.
- **Software transparency and monitoring**: Maintain a comprehensive software bill of materials (SBOM) for relevant tools and dependencies. Monitor for vulnerabilities and apply updates or patches in a timely manner. Where appropriate, consult IT or cyber security colleagues for support and guidance.
- **Isolation and segmentation**: Contain untrusted or high-risk components through approaches such as containerization, sandboxing, and network segmentation to reduce potential impact on core preservation systems.
- **Contractual security requirements**: Include explicit security obligations within service level agreements (SLAs), contracts, and licensing agreements, including audit rights, breach notification requirements, and data portability clauses.
- **Diversity and exit planning**: Avoid single points of dependency by maintaining options for data migration and replacement of critical tools if a supplier, service, or project becomes unavailable. Regularly test exit strategies and document migration pathways.
- Further guidance is available in the DPC Procurement Toolkit (DPC, 2022c).

1.7 AI Security

1.7.1 Repository scraping

The emerging threat of large-scale automated scraping of the Web (and digital collections) was highlighted in the first Guidance Note in this series (‘Understand Cyber Threats’). Mitigating this risk requires a combination of technical controls, clear policies, and community engagement measures:

- **Rate limiting and access controls**: Restrict the frequency and scope of automated access requests to repositories.

- **Monitoring and alerting**: Detect unusual access patterns that may indicate scraping activity or abuse.
- **Clear terms of use and licensing**: Define permitted uses of digital content and communicate expectations clearly to authorized users.
- **Community advocacy**: Engage with wider networks to promote ethical AI practices and encourage responsible access to digital collections. The DPC beginner's guide to Computational Access includes further useful guidance and practical examples on the use and licensing of digital content (DPC, 2022b).

1.7.2 AI in preservation tools

AI is increasingly embedded within preservation workflows, including OCR, format identification, metadata generation, and content analysis. While these tools can significantly improve efficiency and enable new capabilities, they also introduce several inherent risks, including limited transparency and opacity, bias, and potential vendor lock-in.

The use and benefits of AI in digital preservation practice are active areas of discussion within the community. As a general principle, AI components should be treated as high-risk dependencies and managed accordingly. Organisations should adopt appropriate mitigation strategies including:

- **Transparency and documentation**: Ensure AI processes, models, configurations, and outputs are clearly documented within preservation workflows.
- **Human review**: Validate AI-generated outputs through expert oversight and appropriate "human-in-the-loop" review mechanisms before they inform preservation decisions or user access.
- **Data portability**: Maintain the ability to extract, migrate, validate, or replace AI-generated metadata, models, or derived content, where appropriate.
- **Risk awareness**: Include AI components within supply chain and dependency risk assessments, recognising the potential for technical, legal, and operational vulnerabilities. Follow relevant best practice guidance on AI security from reputable authorities, such as the National Cyber Security Centre in the UK and the AI Safety Institute.

A more in-depth discussion of AI and digital preservation can be found in the DPC's Technology Watch Report on this topic (Farquhar, forthcoming).

1.7.3 Threats to authenticity

In addition to cyber security risks, AI technologies such as deepfakes and synthetic media pose challenges to the trustworthiness, authenticity, integrity, and provenance of digital content. Community and standards-based responses are emerging, including Content Credentials initiatives. Professional networks provide valuable guidance and support in navigating these challenges. These issues represent a significant area of ongoing development and will be explored in more detail through future work.

2 Getting Started: A Practical Roadmap

Taking this information together, and particularly if practitioners are approaching the challenge of cyber security for digital preservation for the first time, a suggested sequential roadmap for practical implementation is laid out below. Resources for further guidance are included. Roadmap progress could be cross-referenced against established digital preservation requirements resources and

standards such as EOSC EDEN, CoreTrustSeal and the DPC Core Requirements (EOSC EDEN, 2025; CoreTrustSeal, 2026; DPC, 2022a).

2.1 Phase A – Laying the Foundation (0 to 6 months)

- Refer to key messages and frameworks in the second Guidance Note in this series ('Engage Stakeholders') and work to collaboratively **agree senior responsibility** for preservation cyber security: ensuring authority, accountability, and access to necessary resources.
- Consider the number, location and storage type of existing **independent copies** of the collection, and whether further resilience is required (Wheatley, 2025).
- Advocate for and receive, as a minimum, basic **cyber security awareness training** for staff involved in preservation workflows.
- Work with IT colleagues to:
    - conduct a comprehensive **inventory** of preservation systems, tools, and dependencies.
    - implement **multi-factor authentication,** including for remote access, and maintain offline or geographically distributed backups alongside existing independent copies to protect critical data (NCSC, 2024).
    - Document key incident contacts and establish **clear reporting channels** for cyber incidents. Preservation staff should know how and where to report any usual or suspicious activity. Ensure these procedures are integrated into business continuity planning.
    - **Review lessons learned** from cyber incidents affecting the sector and ensure appropriate preventative and recovery measures are in place (British Library, 2025). **While it is not possible to prevent every cyber-attack, organisations should have well-defined procedures for responding to and recovering from incidents**.
    - Follow current cyber security guidance and best practices. **Identity the national technical authority in your jurisdiction** (for example the National Cyber Security Centre in the UK) and review its guidance with colleagues alongside advice from other reputable sources. This should include keeping up to date with guidance on responding to AI-accelerated cyber-attacks (CSA, 2026).

2.2 Phase B – Building Capability (6 to 18 months)

- Plan a business case for a multiple-copy storage design, using findings from Phase A.
- Work with IT colleagues to:
    - Introduce **network segmentation** and **enhanced monitoring** to isolate high-risk systems and detect anomalous activity.
    - Formalize **secure handling procedures** for removable media, high-risk file formats, and unprocessed collections.
    - Conduct structured **due diligence and security reviews** of vendors, cloud providers, and open-source dependencies, covering:
        - **Technical security:** patch management, access controls, encryption, logging, network protections.
        - **Operational resilience:** backups, disaster recovery, incident response, and change management.
        - **Legal & compliance:** data sovereignty, contracts, licensing, and regulatory requirements.

        - **Governance & organizational practices:** security policies, staff training, transparency, and supplier track record.
        - **Open-source dependencies:** project activity, code quality, licensing, software provenance, and supply chain risks. Where possible, request and review a Software Bill of Materials (SBOM) to understand software components, dependencies, and potential vulnerabilities.
        - Refer to the second Guidance Note in this series *Engage Stakeholders* (section 4, 'Working with IT') for frameworks that can support these assessments.
    - Run regular **incident response exercises**, including scenario-based tabletop exercises, to test preparedness, executive decision-making, and communication pathways (ASD, 2024; ENISA, 2026). These exercises should be viewed not only as a means of testing response capabilities but also as valuable team-building opportunities that strengthen cross-functional collaboration and clarify roles and responsibilities before an incident occurs.

Some of these activities may be undertaken independently by preservation practitioners, while others may be delivered as part of standard central IT processes or through collaboration between both groups. This checklist is intended as a starting point to ensure that appropriate cyber security measures are considered and brought within scope of digital preservation good practice.

2.3 Phase C – Achieving Maturity (18 months and beyond)

- Implement any **required changes** to storage architecture and replication strategies identified in Phase B planning.
- Work with IT to:
    - Embed cyber security practices fully into all preservation workflows, ensuring security is part of **routine day-to-day operations rather than treated as an afterthought**.
    - **Automate** monitoring, integrity checking, and anomaly detection where appropriate to improve efficiency, support proactive risk management and reduce human error.
- Share lessons learned, good practices, and innovations with the **wider digital preservation community** to strengthen collective resilience.
- It may also be worthwhile pursuing **external assurance or certification** to demonstrate robust governance and operational standards. An example would be CoreTrustSeal (CoreTrustSeal, 2026).

By following this roadmap, alongside current guidance and best practices from national technical authorities, organizations can progress from initial awareness and foundational controls through to mature, embedded cybersecurity practices that are fully integrated into digital preservation operations.

3 Conclusion

Cyber security and resilience for digital preservation is complex, but it cannot be ignored. Effective preservation depends upon informed and managed risk-taking: security measures should enable safe and sustainable practice, not prevent it. Success requires collaboration across disciplines, supported by strong leadership, effective governance, and sustained organizational commitment. Regardless of current maturity, every organization can take meaningful steps to improve resilience.

We hope this series of Guidance Notes provides practitioners with a practical foundation to begin this journey and develop their organization's capability in this important area.

There is much we can do to support one another. While cybersecurity is necessarily a sensitive area, and information-sharing must be handled carefully, there remain many opportunities to share good practice, common challenges, principles, and lessons learned for the benefit of the wider community. This promotes community knowledge sharing *and* resilience in all its forms. The transparency demonstrated by the British Library in the wake of its damaging 2023 cyber-attack provides an example of strong and courageous leadership through open communication and information sharing, helping others learn from the incident and reduce the likelihood of similar events (British Library, 2025). Practitioners are encouraged to make use of existing digital preservation networks to connect with peers, share experiences and collectively stay ahead of emerging challenges (GRIN, 2026).

Protecting irreplaceable digital collections from cyber threats is a fundamental stewardship responsibility. This guidance provides a foundation, but the real work takes place in daily practice, as practitioners make informed decisions, build trusted relationships with colleagues across their organization and in the wider community, and continually strengthen their capabilities and resilience. To conclude, the following cyber governance principles for digital preservation summarize some of the key points from these Guidance Notes and are intended to help practitioners ensure that cybersecurity within their own organizational environment supports and enables effective long-term preservation practice.

3.1 Code of Practice: Cyber Governance for Digital Preservation

1. **Cyber security is integral to preservation practice**
   Security should be embedded into all preservation activities and not treated as an external constraint. Effective cybersecurity enables the safe, sustainable, and trustworthy stewardship of digital collections.

2. **Risk is managed, not eliminated, in pursuit of long-term access**
   Digital preservation inherently involves uncertainty and managed risk. Organizations should adopt proportionate, risk-based approaches that balance security, usability, access, and preservation objectives.

3. **Preservation systems require strategic oversight**
   Repositories, storage platforms, and preservation processing environments constitute critical organizational infrastructure. They require awareness at senior level, clear leadership responsibility, and sustained resourcing. Zero Trust thinking can reduce technical risk while supporting a culture of trust and professional responsibility.

4. **Responsibility for cyber security is shared across preservation, IT, and security teams**
   Effective cyber governance depends upon collaboration across disciplines. Clear roles and shared accountability enable secure and efficient preservation workflows.

5. **Supply chain risks are actively governed**
   Dependencies on software, cloud services, hardware vendors, and open-source communities introduce potential vulnerabilities and operational risks. Organizations should proactively assess, monitor, and mitigate supply chain risks throughout system lifecycles.

6. **Staff are trusted, trained, and supported**
   People are central to effective security. Staff should be empowered to exercise professional

judgement, receive appropriate training, and have access to resources and support required to work safely and innovatively.

7. **Continuous improvement is essential**
   Cyber threats, technologies, and preservation practices continue to evolve. Organizations should foster cultures of learning, review, testing, and adaptation to maintain long-term resilience and operational effectiveness.

4 Glossary

Authenticity: That information contained within digital content remains trustworthy**.**

Containerization: A method of packaging applications and their dependencies into lightweight, portable containers that can run consistently across different computing environments (e.g. using Docker).

Encryption: A security process that converts readable data (plaintext) into unreadable code (ciphertext) using algorithms and keys, so that only authorized parties can access the original information.

Integrity: That information contained within digital content remains accurate and complete.

Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to systems. Examples include viruses, worms, ransomware, spyware, and trojans.

Multi Factor Authentication: An authentication system that requires more than one distinct authentication factor for successful authentication.

Network segmentation: Security approach to break a computer network down into smaller networks. This allows stronger control over user traffic flows, and what access is allowed between different networks.

Ransomware: A type of malware which prevents access to devices and data stored on these, usually by encrypting files. A criminal group will then demand a ransom in exchange for decryption.

Rate-limiting: means to limit access to bulk datasets, for example via an API.

Read-only: Read-only refers to a state or mode where you can view or access information, but you can't modify or write new data. In computing, read-only refers to a file, directory, or storage medium that can be accessed and read but cannot be changed or deleted. This attribute is often set to protect critical system files and data from accidental modification or deletion.

Sandbox: An isolated and controlled environment used to safely test software or analyse suspicious files without affecting the main system.

Software Bill of Materials (SBOM): A comprehensive listing of component parts and software dependencies of a software package, designed to help users, vendors and developers better understand the open-source and third-party components it may contain. This should be an exhaustive list which includes open-source libraries, proprietary software, and licensed dependencies. Some may also include the tools used to produce the software, along with other provenance information.

Zero Trust: a series of technical architectural principles, summarised as ‘never trust, always verify’, well suited to designing and managing digital preservation environments and workflows.

5 References

Australian Signals Directorate (2024) 'Cyber security incident response planning: Practitioner guidance' Canberra: 2024. Available at: https://web.archive.org/web/20260607015031/https://www.cyber.gov.au/business-government/detecting-responding-to-threats/cyber-security-incident-response/cyber-security-incident-response-planning-practitioner-guidance

British Library, (2025) *Learning lessons from the cyber-attack.* London: British Library. Available at: https://web.archive.org/web/20260710000158/https://www.bl.uk/stories/blogs/posts/learning-lessons-from-the-cyber-attack

Community Owned digital Preservation Tool Registry (COPTR) (n.d.) Available at: https://web.archive.org/web/20260729104512/https://coptr.digipres.org/Main_Page

CoreTrustSeal, (2026). Available at: https://web.archive.org/web/20260728053115/https://www.coretrustseal.org/

Cloud Security Alliance (2026) *Hardening Your Network Against AI-Accelerated Attacks*. Available at: https://web.archive.org/web/20260716184517/https://cloudsecurityalliance.org/artifacts/preparing-your-networks-for-the-ai-storm

Digital Preservation Coalition (DPC), (2022a). *Core Requirements for a Digital Preservation System.* London: DPC. Available at: https://web.archive.org/web/20260120084848/https://www.dpconline.org/docs/digital-preservation/procurement-toolkit/2581-core-requirements-for-a-digital-preservation-system-v1/file

Digital Preservation Coalition (DPC), (2022b). *Computational Access: A beginner's guide for digital preservation practitioners*. London: DPC. Available at: https://web.archive.org/web/20260727230021/https://www.dpconline.org/digipres/implement-digipres/computational-access-guide

Digital Preservation Coalition (DPC), (2022c). *Digital Preservation Procurement Toolkit.* London: DPC. Available at: https://web.archive.org/web/20260722151002/https://www.dpconline.org/digipres/implement-digipres/procurement-toolkit

Digital Preservation Coalition (DPC), (2023). *Digital Preservation Business Case Toolkit v2.0.* London: DPC. Available at: https://web.archive.org/web/20260714185759/https://www.dpconline.org/digipres/implement-digipres/business-case-toolkit

EOSC EDEN, (2025). *M1.1 Report on Identification of Core Preservation Processes: Design, Guidance and Summary of Findings.* Brussels: EU. Available at: https://web.archive.org/web/20260623172212/https://zenodo.org/records/16992452

European Union Agency for Cybersecurity (ENISA), (2026). *The ENISA Cybersecurity Exercise Methodology.* Brussels: EU. Available at: https://web.archive.org/web/20260729105710/https://www.enisa.europa.eu/publications/the-enisa-cybersecurity-exercise-methodology

Farquhar, A. (forthcoming). *AI and Digital Preservation*. DPC Technology Watch Report, London: DPC.

Global Resilient Information Network (GRIN), (2026). Available at: https://web.archive.org/web/20260701125434/https://www.kb.nl/grin-global-resilient-information-network

Jackson, A. (2026a). 'DigiPres Workbench'. DPC. Available at: https://web.archive.org/web/20260622165040/https://www.digipres.org/workbench/

Jackson, A. (2026b). 'DigiPres Sandbox'. DPC. Available at: https://web.archive.org/web/20260729110304/https://www.digipres.org/workbench/tools/sandbox

National Cyber Security Centre (NCSC), (2024). 'Ransomware-resistant backups'. London: 2024. Available at: https://web.archive.org/web/20260729110425/https://www.ncsc.gov.uk/collection/ransomware-resistant-backups

Open Preservation Foundation (OPF), (2026). 'Viper: Virtual Preservation Environment for Research'. London: OPF/DDHN. Available at: https://web.archive.org/web/20260729110759/https://viper.openpreservation.org/

PREMIS Editorial Committee, (2015). *PREMIS*. Library of Congress: Washington DC. Available at: https://web.archive.org/web/20260706211810/https://www.loc.gov/standards/premis/

Wheatley, P., (2025). *A Risk Driven Approach to Bitstream Preservation.* Version 1.3. DPC Technology Watch Guidance Note, London: DPC. Available at: https://web.archive.org/web/20260309073104/https://www.dpconline.org/docs/technology-watch-reports/2793-bitstreampreservationrisk/file