

Digital Disaster Risk Management for Repositories and Archives

Annette Mills, Collection Development Leader, City of
Charles Sturt and Dr Heather Brown, Librarian, Education
and Sector Standards, Australian Library and Information
Association

**DPC Technology Watch
Guidance Note**

September 2026



DigitalPreservationCoalition

© Digital Preservation Coalition 2026 and Annette Mills and Dr Heather Brown, 2026

ISSN: 2048-7916

This work is licensed under [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/)

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>

1 Introduction

Digital repositories and archives play a critical role in preserving long-term access to the cultural memory and evidence contained within their significant resources. They can vary enormously in size and scope from large international data centres and national repositories to specialist or small community archives. Their digital contents may range from digital research outputs, to contemporary and historical records, to audiovisual and digitized cultural heritage materials.

Yet, all the work that is undertaken in appraising, managing, describing, curating, preserving and delivering digital content can be disrupted or even instantaneously destroyed by a disaster. Furthermore, the likelihood and consequences of disasters are increasing in severity due to two major factors: climate change and cyberattacks. Climate change and disaster risks are escalating and becoming increasingly complex and interconnected. Glasser ([2019](#)) characterizes this period as the ‘era of disasters’ that can have wide ranging impacts that intersect at multi-levels. From a macro-level perspective, climate change is transforming the frequency and severity of disasters such as fires, hurricanes, and floods that can disrupt or destroy digital repositories and archives. A micro-level insight is provided by Tansy’s ([2024](#)) perspective on how climate change can lead to disruption in electric grid stability, impeding access to vital records that must be accessed during emergencies.

Parallel to the risks generated by climate change are the critical risks posed by cyberattacks and the use of ransomware ([Lowrie and Stewart, 2026](#); [Wheatley, 2025](#)). These can be exacerbated by artificial intelligence (AI) that can increase the speed, frequency, and scale of ransomware attacks ([Irshaad and Thembekile, 2024](#)). A related factor is geopolitical uncertainty, as noted by Kilbride ([2023](#)) in his comments on the risks of armed conflict where digital records of government and state institutions become vulnerable to cyberattacks. The cyberattacks on the British Library ([2024](#)), and the Internet Archive ([Pallardy, 2024](#); [Messarra, Freeland and Ziskina, 2026](#)) have highlighted that disasters affecting digital repositories of all sizes can lead to extended disruptions, even when parts of the digital collections remain unharmed.

Overall, the trend of ‘faster disasters’ that are escalating with climate change and cyberattacks underscores the importance of proactive disaster risk management – before, during and after a disaster – to strengthen the resilience of digital repositories and archives.

1.1 Disaster risk management and disaster plans

Disaster risk management (DRM) is defined as ‘the application of disaster risk reduction policies and strategies to prevent new disaster risk, reduce existing disaster risk and manage residual risk, contributing to the strengthening of resilience and reduction of disaster losses’ ([United Nations Office for Disaster Risk Reduction \(UNDRR\), n.d.](#)).

More specifically, the term ‘disaster plan’ is applied to the documented set of procedures and protocols to be followed by an organization to prevent or minimize the risk of a disaster occurring, and describe actions to be taken should a disaster occur ([Australian Library and Information Association \(ALIA\), 2019a](#)).

Disaster risk management for physical collections and associated disaster plans have been well established for several decades, and they can provide a useful model for digital disaster plans, as discussed below in 2.2 and 2.5.

2 An interconnected approach

Building resilience through digital disaster risk management is more than a technical issue; it requires an interconnected approach – using what O’Connor ([2022](#)) terms ‘an interconnectivity lens’

to promote a common understanding and to align digital disaster risk management with the wider organizational and disaster ecosystem. Some key aspects of an interconnected approach are briefly described in the sections that follow.

2.1 Using common terminology

Commonly understood terminology can facilitate interconnecting and coordinating digital disaster risk management across the whole inter-agency disaster ecosystem.

In the context of digital repositories and archives, Saffady (2020) provides tailored definitions of relevant information terms that facilitate shared understanding. They are summarized in the following table:

Term	Definition
Risk (to information)	A combination of threats, vulnerabilities and consequences related to creation, collection, ownership, retention, retrieval and disclosure of information.
Threat	A circumstance, action, or event that poses a danger to an organization's information assets, or that otherwise impairs an organization's ability to achieve information-dependent objectives.
Vulnerability	A weakness that a threat can exploit to damage or compromise an information asset.
Consequence	A negative outcome that results when such exploitation occurs.

2.2 Using commonly understood stages

Using a framework of commonly understood disaster management stages can improve disaster risk management and coordination across multiple organizational levels and agencies. The four interdependent stages of *prevention*, *preparation*, *response* and *recovery* are widely used in the disaster literature relating to digital archives and repositories as well as physical collections (Brown, 2021; [International Council on Archives \(ICA\)](#), n.d.), and likewise used by emergency service organizations ([Australian Institute of Disaster Resilience](#), 2019).

Term	When	Description
Prevention	Before	Involves assessment of digital disaster risks and developing strategies to mitigate the risks. The goal is to reduce vulnerability before a crisis happens.
Preparation	Before	Includes developing a digital disaster plan and staff training. The level of detail in the disaster plan, and the specific risks addressed should be appropriate to the archive or repository's purpose, service expectations and location.
Response	During	Includes the immediate actions during a disaster event and involves ensuring human safety, contacting emergency services, stabilising critical infrastructure, early-stage damage assessment, and taking steps to

		minimise the consequences. This is where coordination and speed are critical.
Recovery	After	Includes the steps taken to minimise the disruption and return of digital repository services to as near as ‘normal’ as possible, together with integrating lessons learned to improve future disaster resilience.

2.3 Integrating with the organization’s strategic framework

Whether archives and repositories are autonomous organizations, or parts of broader institutions, a useful way of strengthening the effectiveness of their digital disaster risk management approach is to strategically align and integrate it into the organizational strategic framework ([ALIA](#), 2019a). This can help to increase the visibility of digital disaster risk management across the whole organization, providing an opportunity to elevate organizational recognition, sustainability and resourcing. As Wheatley ([2025](#)) observes, ‘highlighting the impact of possible loss of content, financial cost and reputational damage can be a powerful way to get senior managers onside’.

Overall, the approach of embedding digital disaster risk management into organizational strategic planning, business continuity planning, risk registers, cyber security practices, and technology lifecycle management strengthens disaster resilience.

2.4 Integrating and clarifying roles and responsibilities

Responsibilities related to digital repositories and archives are frequently distributed across various parts of an organization, often resulting in a siloed approach. Traditionally, archive and repository teams are responsible for establishing preservation priorities, while IT departments focus on managing technology and security. Senior management, in turn, is tasked with establishing governance frameworks, which include setting the organization’s risk appetite and ensuring compliance with relevant policies and regulations.

Interconnecting digital disaster risk management involves clarifying where these responsibilities intersect, in order to coordinate effectively for the best outcome in a stressful situation. It also requires defining stewardship and operational responsibilities, establishing a clear hierarchy (or command structure) for roles and responsibilities and decision making. This should be agreed upon and documented in the disaster plan.

2.5 Interconnecting with physical disaster risk management

As another layer of context, some digital archives may be part of a broader collection that includes physical objects, some of which may have been digitized, and some of which may also have separate disaster plans. It may be helpful to consider if there are benefits in aligning the digital and physical disaster plans for a holistic ‘one stop shop’ approach ([ALIA](#), 2019a; Brown, 2021; UNESCO, [2024](#)).

3 Prevention: assess risks rather than assume resilience

Risk assessment underpins the prevention stage of disaster risk management. The DPC Handbook ([n.d.](#)) provides a valuable overview of risk and change management and its close connection to business continuity planning.

Digital repositories and archives are set up in different ways, however several common risk areas include:

Infrastructure and platform risks: Legacy systems and complex network architectures increase vulnerability to cyberattacks and can significantly complicate and increase the cost of post incident recovery. Ageing systems can weaken monitoring, enable lateral movement by attackers (Baker, 2025), and prevent timely restoration ([British Library](#), 2024).

Backup risks: Small community digital archives may lack reliable backup arrangements. Backups need to be frequent, secure, and held in another location. Backup arrangements, contacts, and locations should be confirmed and documented in the disaster plan. Further details about backups are provided below in the section on replicating digital content.

Power and utilities failure: Adding to Tansy's ([2024](#)) observations on climate change and power grid instability, the risks of electrical outages, whether brief or extended, can cause system shutdowns, data corruption, lost logs, failed backups, and damage to storage or cooling systems. Even if digital content remains intact, power loss can compromise authenticity, delay recovery, and increase security risks. Regular testing of power resilience, backup reliance, and post-outage validation is essential.

Preservation and integrity risks: Even where secure backups exist, each dataset must be validated before restoration. Disasters may destroy logs, audit trails, or fixity evidence, undermining confidence in restored content.

Organizational and capability risks: Recovery often depends on key specialist knowledge that may be concentrated within a small number of staff and/or external suppliers and experts. Capacity constraints can delay rebuilding and validation work and recovery may focus on restoration of services rather than preservation requirements.

Third-party and access risks: Supplier access, particularly where multi-factor authentication is absent, represents a significant attack pathway. Third-party access arrangements should be explicitly addressed as part of the disaster risk management approach and documented in the disaster plan.

The next step is **risk mitigation** - finding ways to reduce or eliminate the risks. Risk mitigation actions may include some or all of the following and can be summarized in the digital disaster plan:

- Replicating digital content in one or more geographic locations (backups) with a differing risk profile. A useful model is the '3-2-1' copy rule: three copies of each file, on two types of storage media, with at least one copy offsite ([Digital Preservation Coalition](#), 2026). The standard ISO/DIS 16363 *Audit and certification of trustworthy digital repositories* (5.2.4, [2025](#)) additionally recommends that a copy of the disaster plan should be stored offsite.
- Implementing cyber security measures such as multi-factor authentication on all internet-facing systems
- Maintaining up to date digital inventories ([Blue Shield UK](#), 2026)
- Implementing network segmentation ([Cisco](#), 2026)
- Implementing immutable and air-gapped backups ([Jehs](#), 2025)
- Avoiding dependence on a single third-party vendor (e.g. cloud storage provider) ([Wheatley](#), 2025)
- Documenting storage management procedures in the disaster plan
- Reporting on the progress of implementing risk mitigation processes to senior management

- Making contact with emergency services who may also be able to advise on aspects of risk mitigation
- Reviewing and testing the mitigation actions and the disaster plan ([Wheatley, 2025](#)).

3.1 Risk assessments

A risk assessment identifies the types of risks that are relevant to the digital repository or archive and then considers the likelihood or probability and the consequences. The risk assessment provides the evidence that shapes the contents of the disaster plan: for example, the risks of a small community digital archive will be different to those of a digital repository at a large university. Risk assessment tools provide standard checklists and risk matrices that can be used to identify and rate the risk level. To be effective it should align with the parent organization's risk management framework. Some readily available tools include the ALIA Guide which provides a simple example ([ALIA, 2019a](#)) and The National Archives UK prototype DiAGRAM tool (Digital Archive Graphical Risk Assessment Model) designed to statistically quantify threats and model outcomes ([The National Archives, n.d.](#)).

While a simple risk assessment can be sufficient to guide consideration of acceptable or unacceptable risks, 'it needs to be comprehensive in scope and an honest assessment of the threats, the likelihood of their realization and their postnatal impact' ([Wheatley, 2025](#)). In practice, the risk assessment process will involve identifying the scope of the risk assessment, discussing the likelihood of potential threats with key staff, checking the digital infrastructure and storage - including backups, and documenting any existing mitigation strategies and further steps that are needed to address significant residual levels of risk ([Wheatley, 2025](#)).

The disaster that occurred in the OVHcloud data centre provides a case study for the role of risk assessments. In this case, if there had been a comprehensive risk assessment undertaken of the data backup arrangements, the assessment would have identified the vulnerability of the backups being stored onsite and recommended an offsite alternative as risk mitigation. Unfortunately, a massive fire destroyed the data as well as the onsite backups ([CentrixIT, 2025](#)). In a similar case in South Korea, a devastating fire in a government data centre destroyed a large portion of government datasets. Van der Schyff ([2026](#)) reports that parts of the system had no effective backup and highlights the organizational risks 'when records are permanently lost, accountability and continuity are damaged long after the crisis has passed'. Further insights into fire risks in data centres are provided by Kareck et.al. ([2026](#)).

Where risk assessment outcomes are documented and connected to the organization's strategic risk management framework, the digital risks become visible at senior management level. This alignment also helps to ensure that digital disaster risk management is recognized as an organizational risk that becomes embedded in planning and policy, as opposed to viewing it as simply a technical issue.

4 Preparation

Preparation involves steps such as compiling a list of emergency contacts and arranging a multidisciplinary disaster team. The disaster team will ideally include roles for a senior or team leader, with the authority to make decisions, a collection specialist (with knowledge of the repository resources and preservation requirements), technical digital specialist, record keeper, and media liaison person. Examples of disaster team roles are provided in the ALIA Disaster Template Part 2 Table 7 ([2019b](#)). Clear definitions of disaster team roles and responsibilities ensure that all relevant parties understand their roles during an incident and can adapt and work together

effectively across different sections to achieve the best possible outcome. Effective disaster preparedness for digital repositories is based on a shared understanding of roles and priorities rather than extensive procedures. Staff training is an important feature of preparation and it is important to practise scenarios where infrastructure could be unavailable for months rather than days.

Another feature of preparation may include identifying and agreeing on digital repository priorities and this is likely to depend on the digital storage architecture. For example, different content and data types received through specific workflows and channels may be stored separately. This could include born digital research data, digitized physical files, harvested web archives, corporate business records, large audiovisual files or geospatial data. In such cases the priorities and associated storage and backup arrangements should be documented in the disaster plan.

Preparation can also involve assembling a disaster store of emergency equipment and supplies. These supplies can include rolls of plastic, torches and personal protective equipment (PPE) that are traditionally held in a physical disaster store, and they can also be useful for protecting onsite digital infrastructure. For example, plastic sheeting can be used to shield server racks or network switches from overhead water leaks or fire sprinklers; PPE and torches can allow response teams to safely access dark or compromised server rooms during power outages. Deploying fans, mops and sponges from the physical disaster store could help reduce humidity in server environments. A list of emergency equipment appears in the ALIA resources ([ALIA](#), 2019b).

A major component of preparation involves developing a digital disaster plan which should be endorsed by a senior manager. As these plans contain confidential information, their distribution should be restricted to key staff and they should also be available in physical format.

Useful features of a digital disaster plan may include some of the following:

- emergency services contacts
- disaster team contacts
- external supplier contacts
- cyber security contacts and experts
- detailed site floor plans, locations of utilities
- storage management and access arrangements including security and keys
- backup (replication) and storage arrangements, agreements and contacts
- IT frameworks for protection of data
- IT disaster recovery solutions
- priority digital resources and their locations
- for larger organizations - a command structure clarifying roles and responsibilities.

5 Response

The response stage is the third phase of disaster management, following prevention and preparation, and is usually relatively short.

It includes calling emergency contacts and the disaster team leader who will then deploy key members of the disaster team (such as the collection specialist and IT specialist). They will begin assessing the impact of the disaster and start to plan the recovery options, including liaising with backup contacts and cyber security experts. If technical infrastructure for digital preservation is located onsite (servers, tape libraries, external disc storage), the record keeper may begin to take photographs and will document the decisions and recovery procedures followed. These records can provide valuable evidence for assessing the long-term impacts of the disaster and reviewing the disaster plan.

Depending on the scale and the type of a disaster, the disaster team leader and key team members may gain access to the site straight away. The UNESCO toolkit provides a useful overview of how the scale of a disaster can potentially influence the response to a disaster that impacts both digital and physical collections ([UNESCO](#), 2024). For large scale disasters such as a major fire or flood, the emergency services will direct the initial response and decide when the site is safe for the team leader and key team members to enter. In a large disaster, entry to the site may take days or even weeks. The British Library's experience shows that immediate containment can occur on the day a cyberattack is identified, while rebuilding minimal viable infrastructure may take around five and a half months ([British Library](#), 2024).

6 Recovery

Recovery involves taking the steps to minimise the disruption and return the digital repository services to as near as 'normal' as possible. The recovery will be focused on digital collection priorities.

Distinguishing between the re-establishment or restoration of services and the process of recovery is also essential.

Restoration is the process of returning systems or data to a previous state, such as retrieving files from backup, with a focus on technical objectives. This step addresses the immediate need to restore access to critical information and systems.

In contrast, full recovery is a broader process that involves restoring full business functionality, operations, and services after the disruption. While restoration is technical in nature (centered on fixing data and systems), recovery is operational, aiming to enable users and the organization as a whole to resume normal work and activities.

Early restoration of services can help rebuild initial confidence and trust in the archive or repository, as the service is visibly operational once again. However, it is important to differentiate this immediate restoration stage from the comprehensive recovery of services.

Recovery involves thorough testing and validation of the repository, ensuring that copies of collections are verified, by using resources such as existing fixity information to confirm that corruption, change and deletion have not occurred, systems are migrated or replaced as necessary, and may also require long-term rebuilding programs and sustained change management. True recovery represents more than just a return to the previous state; it ensures the repository or archive continues to remain trusted and resilient. Resilience requires an organization to adapt rather than simply rebound to a previous state or maintain the 'status quo'. This enables the organization to continue evolving over time as disruptions and risks change ([Bürger](#), 2026).

Disaster incidents can reveal previously unrecognized risks and vulnerabilities. Therefore, the recovery process should be used to incorporate lessons learned into future planning and periodically

review disaster response plans. This continuous improvement strengthens organizational resilience and preparedness for future incidents. A disaster plan is never a 'set and forget' tool. A disaster plan that remains static, without being improved by lessons learned, rapidly loses its relevance ([UNESCO, 2024](#)).

7 Interconnection and continuous improvement

In a landscape of escalating disasters proactive disaster risk management has become critical to strengthen the resilience of digital repositories and archives. Organizations differ in size and level of development, yet the fundamental approaches for effective disaster management remain consistent. It is crucial that digital archives and repositories are explicitly embedded within an organization's comprehensive risk planning framework. A clear definition of disaster team roles and responsibilities ensures that all relevant parties across the organization collaborate and understand their roles during an incident. Additionally, aligning digital disaster planning with an organization's strategic risk framework and risk management strategies helps to embed digital disaster planning as core business and an organizational priority.

Digital disaster planning is strengthened by interconnecting the four stages of disaster management and integrating several key components: risk management, business continuity, and organizational culture. It is the continuous cycle of **prevention, preparation, response** and **recovery** that ensures that the organization moves from vulnerability to long term digital resilience and strength. Active support and participation from senior management and the active cultivation of risk management practices further support a coordinated response, sustaining the overall effectiveness of digital disaster risk management.

8 References

Australian Institute for Disaster Resilience (AIDR) (2019) *Australian Emergency Management Arrangements*, Australian Institute for Disaster Resilience, Available at:

https://web.archive.org/web/20260907101055/https://www.aidr.org.au/media/7095/aidr_flipbook_emarrangements_2019-08-22_web_v2.pdf

Australian Library and Information Association (ALIA) (2019a) *Disaster management for libraries. Part one: Guide*, ALIA. Available at:

<https://web.archive.org/web/20260729184414/https://read.alia.org.au/alia-disaster-management-libraries-part-one-guide>

Australian Library and Information Association (ALIA) (2019b) *Disaster management for libraries. Part two: Disaster plan template*, ALIA. Available at:

https://web.archive.org/web/20260907101221/https://read.alia.org.au/sites/default/files/documents/alia_disaster_management_for_libraries_-_part_2_template.pdf

Baker, K. (2025) 'Lateral movement explained', *Cybersecurity 101: The Fundamentals of Cybersecurity*, Available at:

<https://web.archive.org/web/20260907101302/https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/>

Blue Shield UK (2026) *Reducing Disaster Impact on Cultural Heritage* [LinkedIn post] 13 May.

Available at: https://www.linkedin.com/posts/blue-shield-united-kingdom_blueshielduk-culturalheritage-disasterriskreduction-activity-7460267639551090691-JVyQ?utm_source=share&utm_medium=member_ios&rcm=ACoAAAKFSf4BO7i8QqYFfklqcf77o4i-6tygK_M [Accessed 7 September 2026]

British Library (2024) *Learning lessons from the cyber-attack: British Library cyber incident review*, British Library. Available at:

<https://web.archive.org/web/20251027163136/https://www.bl.uk/files/v5dwkion/production/99206a2d1e9f07b35712b78f7d75fbb09560c08d.pdf/british-library-cyber-incident-review-8-march-2024.pdf?dl>

Brown, H. (2021) 'Interconnected disaster management: Bridging the physical and digital divide', *Journal of the Australian Library and Information Association*, vol. 70, no. 3, pp.263–286.

Bürger, B. (2026) *What do we actually mean when we say resilience?* [LinkedIn post] 25 May.

Available at: https://www.linkedin.com/posts/bernhardbuerger_what-do-we-actually-mean-when-we-say-resilience-activity-7464555892353466368-hr9b [Accessed 7 September 2026]

CentrexIT (2025) 'When the fire took everything: A data center disaster that destroyed backups too'.

Available at: <https://web.archive.org/web/20260608111750/https://centrexit.com/blog/data-center-fire-destroyed-backups-disaster/>

Cisco (2026) 'What is network segmentation?', Available at:

<https://web.archive.org/web/20260907101703/https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html>

Digital Preservation Coalition (DPC) (n.d.) *Digital Preservation Handbook*, DPC. Available at:

<https://web.archive.org/web/20260829053835/https://www.dpconline.org/handbook/>

Digital Preservation Coalition (DPC) (2026) *Community Archives Digital Preservation Toolkit: Toolkit matrix-make copies*. DPC. Available at:

<https://web.archive.org/web/20260729155143/https://www.dpconline.org/digipres/implement-digipres/community-archives-dp-toolkit/community-archives-toolkit-matrix/community-archives-make-copies/community-archives-make-copies-2>

Glasser, R. (2019) *Special report: Preparing for the era of disasters*, Australian Strategic Policy Institute, Barton. Available at:

https://web.archive.org/web/20260907101845/https://www.aspi.org.au/report/preparing-era-disasters/?_cf_chl_rt_tk=MJDa_q7hYNStkob6nW1HjbheR2vBnGk86uOGHfDX7bl-1788776325-1.0.1.1-vES9OgHPgLVvaSax7ts9STXPTe6qWbsjZ3W9f0p2uM

International Council on Archives (ICA) Expert Group on Emergency Management and Disaster Preparedness (EGEMDP) (n.d.) *Emergency Management and Disaster Preparedness: Mitigation, Preparedness, Response and Recovery*. Available at:

<https://web.archive.org/web/20260907101954/https://www.ica.org/ica-network/expert-groups/egempdp/>

International Organization for Standardization. (ISO). (2025). ISO 16363 Space data and information transfer systems – *Audit and certification of trustworthy digital repositories*. Geneva: ISO. Available at: <https://www.iso.org/obp/ui/en/#iso:std:iso:16363:ed-2:v1:en> [Accessed 7 September 2026]

Consultative Committee for Space Data Systems (CCSDS) (2024) *Recommendation for Space Data System Practices* Available at:

<https://web.archive.org/web/20260425083751/https://ccsds.org/Pubs/652x0m2.pdf>

Irshaad, J. and Thembekile, O. M. (2024) 'Impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review', *Data and Information Management*, vol. 8, no. 2. Available at: <https://doi.org/10.1016/j.dim.2023.100063> [Accessed 7 September 2026]

Jehs, G. (2025) 'Air gap vs immutable backups: Understanding the difference between air gapping and immutable storage', *Meridian IT*, 7 February. Available at:

<https://web.archive.org/web/20260907102329/https://www.meridianitinc.com/blog/difference-between-air-gapping-and-immutable-storage>

Kareck, T.L., Li, C.-Y., Wang, J., Gollner, M.J. and Wang, Q. (2026) 'From incident to insight: Fire risk in modern data centers', *Journal of Loss Prevention in the Process Industries*, 100, p.105890. Available at: <https://doi.org/10.1016/j.jlp.2025.105890> [Accessed 7 September 2026]

Kilbride, W. (2023) *DP Disrupted: A blue shield for the electronic battlefield*. [Blog], 3 April. Available at: <https://web.archive.org/web/20260615130027/https://www.dpconline.org/blog/dp-disrupted-a-blue-shield-for-the-electronic-battlefield>

Lowrie, H. and Stewart, G. (2026) *Cyber Security and Resilience for Digital Preservation, Part 1: Understand Cyber Threats*. DPC Technology Watch Guidance Note. Available at:

<https://web.archive.org/web/20260907103226/https://www.dpconline.org/docs/dpc-technology-watch-publications/technology-watch-guidance-notes/3635-twgn-cybersecurity-hlgs-part1-understand-final/file>

Messarra, L., Freeland, C. and Ziskina, J. (eds.) (2026) *Vanishing Culture: A Report on Our Fragile Cultural Record*, 2nd edn, Available at: <https://archive.org/details/vanishing-culture-2026/mode/1up>

- The National Archives (n.d.) *DiAGRAM – The Digital Archiving Graphical Risk Assessment Tool*, version 1.0.0 Available at:
<https://web.archive.org/web/20260907103436/https://diagram.nationalarchives.gov.uk/index.html>
- O'Connor, J. (2022) 'Managing disaster risks in an interconnected world', United Nations Office for Disaster Risk Reduction (UNDRR), 12 October. Available at:
<https://web.archive.org/web/20260907103540/https://iddrr.undrr.org/news/managing-disaster-risks-interconnected-world>
- Pallardy, C. (2024) 'Internet Archive Cyberattack Saga Continues', *InformationWeek*, 24 October. Available at: <https://www.informationweek.com/cyber-resilience/internet-archive-cyberattack-saga-continues> [Accessed 7 September 2026]
- Saffady, W. (2020) 'Risk terms and concepts', in *Managing information risks: Threats, vulnerabilities and responses*. Lanham, MD: Rowman & Littlefield, pp.1–25.
- Tansy, E. (2024) *Environmental impact and digital preservation*, DPC Technology Watch Guidance Note. Available at:
<https://web.archive.org/web/20260718142944/https://www.dpconline.org/docs/dpc-technology-watch-publications/technology-watch-guidance-notes/3130-environmental-impact-and-digital-preservation/file>
- UNESCO (2024) *Building resilience: disaster risk management for documentary heritage and digital archives; training toolkit*, UNESCO Office Bangkok and Regional Bureau for Education in Asia and the Pacific, document code BGK/C3-8878/CI/24/017, Available at:
<https://unesdoc.unesco.org/ark:/48223/pf0000391132> [Accessed 7 September 2026]
- United Nations Office for Disaster Risk Reduction (UNDRR) (n.d.) *Sendai Framework Terminology on Disaster Risk Reduction: Disaster risk management*. Available at:
<https://web.archive.org/web/20260829194409/https://www.undrr.org/terminology/disaster-risk-management>
- Van der Schyff, J. (2026) 'South Korea held data domestically-and lost it in a fire', *The Strategist*, 19 January. Available at:
<https://web.archive.org/web/20260707110813/https://www.aspistrategist.org.au/south-korea-held-data-domestically-and-lost-it-in-a-fire/>
- Wheatley, P. (2025) *A risk driven approach to bitstream preservation*, DPC Technology Watch Guidance Note. Available at:
<https://web.archive.org/web/20260903174729/https://www.dpconline.org/docs/technology-watch-reports/2793-bitstreampreservationrisk/file>