Who guards the guards: meeting the challenges of digital preservation

HEATHER BROWN
Assistant Director, Paper, Artlab Australia and Project Officer, State Library of South
Australia for University of S A Business Information Course

Abstract

This paper discusses the importance of preserving digital knowledge over a period of time, the challenges, priorities and the various principles and strategies for long term preservation. It draws on a risk management framework, using the analogy of 'who guards the guards' to explore the implications of dangers, the roles of those who safeguard digital content, and various strategies – technological, resourcing and organizational – for mitigating risks over a period of time. Three key strategies potentially have the capacity to profoundly influence the survival of digital knowledge into the future: collaboration and alliances, risk management and quality assurance, and education and training.

E-mail Brown.Heather@dpc.sa.gov.au

Digital preservation – the 'why'

Preservation links our past with the future.

As the world around us is changing rapidly, one of the few things that will last is the knowledge and cultural heritage that we preserve for future generations, as expressed in the following poem.

Knowledge

Stories can be read
in the mind's eye
without a single step of motion.

Lives live their own stories
within the creation of empires
that disappear on the wings
of distant memories.

What colour once ruled the skies
to be now seen in the horizon
of the setting sun?

Thunder rolls
the troops of conquest
until they become
the dust of another age.

Another face, another stage,
yet the story stays the same;
for what remains is
the breath that gives
the voice to all stories –
knowledge.

(©K S Brown 2005)

A significant part of the world's knowledge and heritage is now in digital form. As UNESCO has recognized in its Charter on the Preservation of Digital Heritage, this needs to be preserved as part of the cultural memory of the whole world (UNESCO 2004).

Allied with the cultural reasons are pragmatic, economic imperatives for preserving digital information. As Lynne Brindley, CEO of the British Library, comments: 'there are sound economic reasons for preserving the 'digital assets' that are resulting from large investments in digitising projects' (Brindley 2000).

Archivists and records managers will also attest that digital preservation is linked to accountability – particularly of governments and organizations. This view is supported by the NSF-DELOS Working Group on Digital Archiving and Preservation: '…we expect this [digital] content will remain accessible to allow us to validate claims, trace what we have done, or pass a record to future generations.'

So for all these reasons, the preservation of digital content is vitally important to our globally-linked, online, 24/7 societies.

The author uses the analogy of the 'troops of conquest' from the poem to symbolise the dangers faced by digital content over a period of time, and will explore the potential implications for the role of 'guarding' this content for the future.

Within this framework, the author uses the UNESCO definition of digital preservation as: 'the processes of maintaining accessibility of digital objects over time' (UNESCO 2003).

Digital content – the what

There are two streams to digital content.

On the one hand there is content that is 'born digital' such as websites and e-mails. On the other hand there is content that is 'turned digital', or copied ('reformatted') to digital, from paper-based, film-based or other analogue media.

In both of these streams, the digital formats and carriers are many and varied, and rapidly increasing in complexity and quantity. The 'bits' and 'bytes' can be delivered via a bewildering variety of magnetic tapes and disks, sound and image files, e-journals and interactive digital maps, databases, web sites and dynamic, mixed-media productions.

Both the sheer scale and variety of digital forms create key challenges for would-be guardians of digital repositories. Robin Dale

has likened the situation to a veritable 'wild west' of different digital repositories with variant file formats and platforms for maintaining and storing digital data (Dale 2006).

The dangers

These challenges in preserving digital content have been evocatively described as 'the digital dark age' (Deegan and Tanner 2002) and 'the dark archival underbelly' of 'the wonderful world of digitised information and online everything.' (US-Inter PARES Project, 2002 Quoting The Boston Globe 10 February 2000, cited in Harvey 2005).

In a nutshell, the 'troops of conquest' have taken on beguiling forms that infiltrate via changes in software and hardware. Furthermore, the old guardianship approach of 'benign neglect' that was previously applied to traditional library materials will not work with digital content. A new approach requiring frequent and active intervention is needed.

An infamous case study is that of the BBC Domesday project which produced a multi-media version of the Domesday Book on videodisc, to mark the 900th version of the original Domesday Book. Unlike the original book that has lasted over 900 years, the videodisc became inaccessible after just a few years in the late 1980s as the BBC microcomputer on which it was developed became obsolete. The data was later rescued using intensive emulation techniques (Abbott 2003).

The lack of reliable data about the costs of preserving digital information provides another set of potential danger.

Jonas Palm, Director, Head of Preservation at the National Archives of Sweden, aptly describes this in an article entitled 'The digital black hole': 'In the excitement about the solutions digitalization offers, the right questions about costs are often not asked, especially about the long term costs for keeping the digital files alive. This enthusiastic attitude is risky, for the conversion process to create the digital files may well be quite expensive to start with, and these investments may turn out to be wasted if planning for the future is ignored and no structural funding for maintenance is secured.… The more information is converted, the more costs for accessing it will go up. The digital black hole has got its firm grip on the project.'

While these are difficult to predict, overall there is a general agreement that they are significant. Jonas Palm clearly highlights that the real costs are in the ongoing management – the costs of 'guarding' the digital content for the future.

The issue of authenticity is another insidious, lurking danger – what attributes of digital materials do we preserve and what level of change, or loss is acceptable? This is particularly a dilemma in the case of 'born digital' material. For example, many websites are dynamic and interactive with 'search and retrieval aspects intrinsically bound up with their content'. However, we need to preserve the functionality of the search and retrieval components, as well as the data that the functionality interacts with to generate the required output (Smith 2003 quoted in Harvey 2005).

Confidence in the authenticity of digital content over a period of time is critical, owing to the ease with which alterations can be made, and the changes caused by processes such as migrating information from one system or carrier to another (UNESCO 2003, p. 113).

It is said that 'trust is like a crystal ball – once it is broken, you cannot fix it'. As India's IGNCA (Indira Gandhi National Centre for the Arts) and NMM (National Mission for Manuscripts) would attest, trust in authenticity is crucial in a country like India, with so much of its cultural heritage contained

within its ancient manuscripts. (IGNCA 2009, NMM 2009).

Allied to trust is the danger that some organizations responsible for digital libraries and repositories will inevitably cease to exist over a period of time, due to funding, political or social changes. Will their digital content be lost? Will it be technically possible to safeguard the content by transferring it to another organization with differing methods of storing and maintaining data? Similar issues are posed by threats of major disasters, terrorism, attacks by hackers or viruses, and civil unrest – particularly as they all affect power supplies and the integrity of buildings.

Another danger is that of ignorance – lack of awareness about the need for pro-active thinking and taking early and repeated actions to preserve digital materials. IT vendors demonstrated this lack of understanding during the BBC Domesday project:

> [one vendor] 'offered us a special polymer that they guaranteed would preserve a CD-ROM [disc] for 100 years. They were unable to answer how we would preserve a CD-ROM player for that length of time…' (Abbott 2003, p. 10)

Lack of established legal frameworks for copying digital materials for preservation purposes are another kind of threat.

'Copyright legislation impacts on the ability of organisations to undertake digital preservation activities. This can affect most areas of digital preservation, including copying and reformatting, preserving and providing long term access to stored material in archives, repositories and libraries. The problem is compounded by the lack of uniformity in copyright laws over various jurisdictions' (PADI 2009). As an example, Australia's Copyright Amendment (Digital Agenda) Act 2000 allows digital copying of materials held in libraries for preservation purposes, but in other countries, commercial imperatives to protect intellectual property rights may override preservation needs. Another layer of complexity is that of copyright in traditional knowledge systems that are embedded in digital objects (Gaur 2009).

A further threat is the imperative of organizations such as libraries and archives to provide access to knowledge and cultural heritage. Access is critical – without it collections are useless. Yet, particularly with 'turned digital' materials, this causes problems when digitization for access is also equated with long-term preservation.

When funding is directed simply to digitization for short-term access without consideration of the bigger preservation picture – including preserving the originals – we are in danger of losing our entire heritage; digital and non-digital.

Paolo Usai, the Director of Australia's Screensound, summed up this danger at an international Web Archiving Conference: 'If there is too much emphasis on access instead of preservation we lose balance and our cultural assets' (National Library of Australia 2004).

What should be kept?

On the other hand, destruction of some aspects of our digital culture is inevitable and even to be welcomed – due to the vast quantity and varying quality of what is created digitally on a daily basis. We simply cannot or even would want to preserve everything.

Ideally selecting for preservation is a pro-active process, involving ongoing interventions to make informed choices about what should travel across time for the benefit of future generations – a survival of the 'culturally-significant'.

According to the UNESCO Guidelines – on one level, the selection of digital heritage is conceptually the same as selection of non-digital material. In the best of worlds, deciding what to preserve should be linked to collection

management priorities and/or archival appraisal criteria and records management policies (UNESCO 2003).

However, on another level, digital materials present some new selection challenges. These include the sheer volume of materials and varying quality, and the complications of new emerging genres, together with the need to act quickly. According to the UNESCO Guidelines: 'It may not be possible to wait for evidence of enduring value to emerge before making selection decisions.'

There is also the challenge of deciding how much to select. In web archiving for example, should the approach be selective as with the National Library of Australia's PANDORA model, or the whole of domain snapshot harvesting of the Internet Archive, or a combination?

It is inevitably a balancing act. While we cannot preserve the whole digital universe, the UNESCO Guidelines suggest that it is probably better to err on the side of collecting more material than less. In selecting for the future the UNESCO Guidelines provide some useful signposts, including the following.

- Decisions should be based primarily on the value of material in supporting the mission of the organization.
- This value must be weighed against the costs and difficulties of preservation and availability of resources.
- It is desirable to preserve at least a sample of all kinds of digital materials, including the clearly ephemeral.

Another helpful resource is the Decision Tree that outlines options and pathways for selecting what to preserve in the DPC Handbook. (DPC 2002)

Whatever the approach, the decision needs to be cautious and taken early for, as the UNESCO Guidelines state, a decision not to preserve is usually a final one for digital materials (UNESCO 2003, p. 75) .

So far, my focus has been on the why and what of preserving digital heritage, and on some of the key dangers. These issues set the scene for the next stage.

Who are the 'guards'?

Traditionally libraries and archives have seen the preservation of resources as a core responsibility, with the librarians, archivists and records managers taking on the role of 'safe-guarding.'

'Society has always created objects and records… and it has consciously preserved them in a permanent way… Cultural institutions are recognized custodians of this collective memory: archives, libraries and museums play a vital role in organizing, preserving and providing access to the cultural intellectual and historical resources of society. They have established formal preservation programs for traditional materials and they understand how to safeguard both the contextual circumstances and the authenticity and integrity of information and objects placed in their care'
(Smith 2002, pp. 133–134).

With digital information, the safeguarding role is expanded to new dimensions. Librarians, archivists, and records managers, the traditional guardians of heritage, will also need to work collaboratively at an international level and intensively with other, newer stakeholders in preserving digital content. (Hoorens 2008). According to UNESCO's Charter on the Preservation of Digital Heritage these newer stakeholders potentially include a diverse team of: 'hardware and software developers, creators, publishers, producers and distributors of digital materials as well as other private sector partners' (UNESCO 2004 Article 10).

While considerable debate has focused on the roles these various stakeholders might take, ultimately it seems probable that digital preservation will be led by those stakeholders

with an interest in or mandated responsibility for preserving knowledge for the future.

So what does this mean for the roles of these new guards? And what does this mean in terms of monitoring their roles, or 'guarding the guards'?

To explore these issues, I now want to turn to the framework of risk management, drawing on the work of Jonathan Ashley-Smith (Ashley-Smith 1999).

Risk management: a framework for 'guarding the guards'

An analogy of risk

The well-known story of the old Indian city of Daulatabad is a powerful reminder about risks, and it is a story that has lessons for all of us who are in the business of trying to preserve knowledge over a period of time. In a nutshell the ruler wanted to build a fort that would safeguard his people – a most trustworthy, impregnable fort, with a huge moat and spikes on the gates to ward off elephant charges. The impregnable fort was invaded – simply – by bribing the guard at the gate.

From a risk-management perspective, the potential dangers outlined earlier are viewed as 'risk factors' and they are then assessed in terms of significance, likelihood and consequences.

Working within this framework we can now turn to some principles and strategies that may help to mitigate the risks and to 'guard the guards.'

Principles and strategies

It is clear that there is no single magic weapon or shield to help solve the complex, challenging problems of digital preservation. It is likely to be a combination of several or all of these strategies integrated into the day to day activities of key command centres, staffed by a wide range of digital stakeholders, that will succeed in achieving some level of risk mitigation.

Standards, guidelines, and preservation metadata

Foremost among these strategies are guidelines and standards that play a key role in reducing the risk of losing digital content. They promote certain common requirements for quality and also make it easier for collaboration and interoperability among organizations.

Good progress has been made in a number of areas. These include identifying and promoting particular formats and features that are likely to make preservation easier – for example the TIFF and JPEG 2000 image file formats. (Buckley 2008). Also useful are the ISO standards for preservation of digital materials (Adelstein 2003) and the UNESCO Guidelines (UNESCO 2003).

OAIS model

Potentially one of the most important frameworks developed to date is the OAIS (Open Archive Information System) reference model. The model is an ISO standard and provides a common framework for describing and comparing architectures and operations of digital archives and is used as the basis for a wide range of digital preservation systems internationally (CCSDS 2002).

Preservation metadata

The concept of preservation metadata underpins this framework. Preservation metadata describes and records information needed to manage the preservation of digital resources; information such as the date of capture, the capture device and change history. The PREMIS metadata model is entwined throughout the OAIS framework and is designed to be applied flexibly across different types of systems (Guenther 2006, Woodyard-Robinson 2006).

This framework has now been developed to enable digital objects to be exchanged in a meaningful way between different platforms

(Raftos 2006). This is a vitally important risk mitigation strategy: for the first time it is now technically possible to safeguard digital content by transferring it to another organization with differing platforms.

Other features – unique identifiers, encapsulation, and others

Linked with the OAIS framework and preservation metadata are other features that help ensure ongoing access to authentic and trusted digital objects.

Among these are the measures for using unique identifiers. These are needed because the current system of identifiers (URLs) is based on file location, and so a change in location means there is a need to change in identifier. Like the gateways themselves, new systems of persistent identifiers are continually evolving; the National Library of Australia has recently adopted a new model of persistent identifiers for its newspaper digitalization project (NLA 2007).

Encapsulation techniques also assist ongoing access, and are linked with emulation. These techniques relate to the packaging together of the digital item, its preservation metadata and other associated data – possibly even the associated software required for access. The packaging process lessens the likelihood that any key component needed to decode a digital object will be lost.

Other measures that can help ensure authenticity include digital watermarking and signatures, encryption, digital time stamping, audit trails, and controlled custody (NSF-DELOS Working Group on Digital Archiving and Preservation, 2003 p. 6).

However, as Cullen points out, while, such strategies improve over a period of time, they may not ensure unconditional authenticity, and he poses the hard question: how confident can one be when an object whose authentication is crucial depends on electricity for its existence (Cullen 2000). Further

research and development is needed in this area of vulnerability.

Auditing and Trusted Digital Repositories

Auditing is a powerful tool for checking the level of risk and 'guarding the guards'. A continuous auditing cycle makes sure systems are working to quality assurance levels and links back to their role in maintaining the identity, integrity, and quality of the digital copy as a trusted source of the cultural record.

A landmark for auditing is TRAC (Trustworthy Repositories Audit and Certification: Criteria and Checklist) produced by OCLC, the Center for Research Libraries and the National Archives and Records Administration. Revised in 2007, this is the first guide for objectively determining whether a digital repository can be a long-term trusted location for digital content.

Not surprisingly, the TRAC Checklist draws on a risk management framework and the OAIS model to identify indicators of trustworthiness and reliability for digital repositories to manage their digital resources to their 'designated communities' now and into the future.

A range of similar auditing tools is emerging, including DRAMBORA (The Digital Repository Audit Method Based on Risk Assessment). DRAMBORA is a toolkit for providing repository administrators with a self-check framework. Similarly, NESTOR, the agency assigned to the task of auditing and certifying digital archives in Germany, has developed its own auditing tools.

As an example of the auditing process in action, during 2009, the Center for Research Libraries audited two repositories with the goal of their certification as trustworthy digital repositories (CRL 2009).

Overall, such a trusted digital repository is 'a complex interrelated system'. (NESTOR 2006).

Key features include: 'the organization running the repository: its governance, organizational structure and staffing; policies and procedures; financial fitness and sustainability; the contracts, licenses, and liabilities under which it must operate; and trusted inheritors of data, as applicable. Additionally, the digital object management practices, technological infrastructure, and data security in place must be reasonable and adequate to fulfil the mission and commitments of the repository' (TRAC 2007 Introduction).

A trusted digital repository will also recognise threats to and risks within its systems and will undergo constant monitoring, planning, and maintenance to carry out its mission of digital preservation.

What is clear is that these complex, interrelated systems will require frequent, ongoing auditing, and that continuing research and development is required to refine the auditing tools for risk analysis.

Refreshing, migrating, emulation – technological strategies

In combination, three key technological strategies are a powerful means of mitigating risk to digital content if they are used within a systematic framework such as the OAIS model.

They comprise:

- refreshing – periodically moving a file from one physical storage medium to another as an ongoing process
- migration – moving files from one file encoding format to another
- emulation – recreating the application environments on which the original files can run.

To make these strategies more effective, new systems architectures and tools such as PANIC and AONS are being developed to automatically detect obsolescence and notify that actions are needed (Hunter 2006).

The European consortium PLANETS is providing a 'test bed', a controlled environment where such strategies and tools can be tested and evaluated (PLANETS 2009).

Microfilm – a prudent option for text-based content

In the case of 'turned digital' content that is derived from text-based materials, another prudent risk management strategy is the so-called hybrid option. A microfilm copy provides for long term preservation, together with a digital copy providing the flexible, multidimensional access.

Microfilm produced and stored to well-established, rigorous international quality assurance standards has a life-expectancy of 500 years.

This hybrid approach meshes with Robin Dale's comments that, as different repositories keep their data in different ways, it is important to use a variety of preservation options within and between organisations (Dale 2006).

The hybrid approach has also been endorsed by IFLA where microfilm has become an integral step in newspaper digitisation programs (IFLA 2002).

From a financial perspective, combining microfilming and digitizing might be seen as costly and unnecessary duplication. The reality is that it provides a flexible, economic coalition. The microfilm copy provides a platform that is low risk and from which it is frequently more cost effective to digitize than from the originals (Brown and Fenton 2005).

Jonas Palm also supports the microfilming option. In The Digital Black Hole he comments that the hybrid solution of COM (computer output microfilm) along with the digital copy may, in financial terms, be a more prudent strategy.

The Swedish National Archives [Riksarkivet] is currently studying whether it is feasible to use COM in an effort to improve the strategy of microfilming, which has a long record for

securing information on materials in bad condition (Palm 2006).

It is also a strategy adopted by the National Archives of Singapore which captures its electronic records and immediately writes them to microfilm as the long term option (National Archives of Singapore 2009).

Legislation

To help get hold of digital materials in the first place a number of countries have, or are currently considering, legal deposit legislation that covers digital materials. New Zealand, for example has passed legislation that 'provides for the deposit for physical format documents and for the copying of internet documents' and Australia is moving in the same direction (Verheul 2006).

Similarly, legislation to allow copying of digital materials for preservation purposes is a key strategy to ensure that vital processes such as refreshing, migrating, emulation are not curtailed by legal requirements.   As the PADI website reports: '…Solutions include introducing licencing for preservation and lobbying governments to change legislation so that there is a balance between the rights of the copyright holders to protect their interests and exemptions for institutions for legitimate long term preservation purposes' (PADI 2009).

Resourcing

As the Cornell Digital Preservation Tutorial highlights, adequate resourcing is just as critical as the technological strategies in ensuring preservation of digital content over a period of time. Building a long term resourcing infrastructure – finding ongoing funding to sustain the guards and systems – is particularly challenging (Shenton 2009). For example, while it is likely that unit data storage costs will decline over a period of time, the overall volume of data to be stored

will continue to grow exponentially in sheer numbers, and as digital objects incorporate more features.

Jonas Palm evocatively describes this dilemma:

'In the excitement about the solutions digitization offers, the right questions about costs are often not asked, especially about the long term costs for keeping the digital files alive. This enthusiastic attitude is risky, for the conversion process to create the digital files may well be quite expensive to start with, and these investments may turn out to be wasted if planning for the future is ignored and no structural funding for maintenance is secured.

Without such long-term planning, digitization projects can come to behave like black holes in the sky' (Palm 2006).

Colin Webb describes how difficult it is to argue the case for ongoing funding to administrators when the long-term costs are unknown. 'To say "we only know it will cost a lot" is an unsatisfactory answer, even if it is the truth' (Webb 2004 p. 45).

However, doing nothing – or paralysis is not an option. Very useful steps for moving forward are outlined in the Cornell Digital Preservation Tutorial including identifying start and ongoing costs. It is often easier to obtain seed money for start up costs. Ongoing costs need to be found from a variety of strategies. At the National Library of Australia, it has been possible to find some funding for ongoing costs by reallocating some priorities and drawing on skills and commitment already in the organization. In Webb's view: 'this has tended to encourage senior managers to pay close attention to digital preservation programmes, and help embed such programmes in the core business of the library.' (Webb 2004 p. 45)

Organizational infrastructure

Organizational infrastructure is equally critical to safeguarding digital heritage. Overall, it involves organizational commitment as reflected through the policies and procedures and the plans for digital preservation. This means writing and supporting, implementing, reviewing and maintaining policies, plans and procedures and getting 'buy in' right from the top. Without this high level commitment, the attempt to guard digital content over time will lack direction and ultimately fail.

Policy direction aligns the strategies for preserving digital information and applies resources where they are most needed. Examples of high level policies and strategies are the National Library of Australia's Digital Preservation Policy and the British Library's Digital Preservation Strategy. India is similarly developing its policies and strategies (IGNCA 2009). Inevitably these will link with selection criteria – the decisions about what to preserve, as discussed earlier. They also deal with roles and responsibilities and managing intellectual property. There are close links with technological infrastructure with requirements for managing quality assurance.

Collaboration

As preservation challenges are the same for everyone in the digital universe, collaboration is a way of sharing expertise in the construction and ongoing maintenance of the gateways. Inevitably these become part of the organizational infrastructure. More formal agreements and collaborations are an important way of sharing development costs, harnessing and focusing effort, and attracting resourcing and support for programs (UNESCO 2003 pp. 64–65).

Examples at the international level include alliances and services such as ICADS (a joint alliance of IFLA and the Conference of Directors of National Libraries), UNESCO, OCLC, PADI, PLANETS, The Internet Archive and The International Internet Preservation Consortium. Verheul highlights many such examples at regional and national levels in the 2006 IFLA survey Networking for Digital Preservation (Verheul 2006).

However, while collaboration and alliances are beneficial, they also cost and need ongoing commitment. As Webb comments: 'the most effective collaboration programmes seem to have been based on areas of real common interest, realistic expectations, clear understanding about who is responsible for what, and the allocation of sufficient resources to pay attention to the collaborative relationship itself' (Webb 2004).

Education and training

Training in quality assurance and in preservation strategies – training the guards and other stakeholders – is a fundamental risk management strategy. It impacts directly on monitoring the auditors or 'guarding the guards'.

Whole new skill sets are needed by digital librarians and other stakeholders to develop and sustain digital preservation. Not only do the new guards need an awareness of the challenges and technological knowledge, they also need more generic skills that particularly impact on the organizational and resourcing infrastructure, skills such as project management and communication skills and the ability to adapt to change. They also need vision and critical thinking skills together with the knowledge and ability to deal with technological challenges; to proactively select, intervene, and to collaborate across boundaries in order to build preservation and sustain gateways for the long term.

The challenge is for the universities and educators of librarians to provide the relevant foundation of knowledge and skills, and for digital library staff to continue to develop and

adapt their knowledge and skills as part of their life-long learning. (Rasmussen and Youngok 2006).

Education and training can take the form of formal qualifications, workshops, short courses, conferences and self-learning, and all have their place in the continuous learning spectrum.

An example of a well established formal training programme is HATII (the Humanities Advanced Technology and Information Institute) at the University of Glasgow that offers a Masters in Information Management and Preservation – with a focus on digital preservation (HATII 2009).

As an example of formal training within Australia, I am currently involved in developing part of the new BIM (Business Information Management) Course at the University of South Australia that is taking an innovative approach. Recognising that the information world is one of constant change and blurring boundaries of responsibility, the new program integrates the areas of archives, records management, knowledge management, librarianship and business information. The aim of the course is to develop awareness of a wide range of stakeholders to key issues in information management such as digital preservation, which are considered within a risk management framework (University of South Australia2009). More formal programmes like these are needed across the region.

As an example of a workshop model within the region, the National Archives of Singapore continues to provide leading-edge training workshops to regional colleagues about digitizing and microfilming quality issues to practitioners and project managers, focusing on the risks and benefits of different approaches.

As examples within India, DELNET plays a leading role in providing training and professional development to library staff – including digital preservation (DELNET 2009).

Likewise, the ICDL Conference on digital libraries is increasingly addressing issues of digital sustainability and preservation (ICDL 2006).

To complement these, a wide range of training courses are now available that not only raise awareness of quality issues but also highlight the risks in preserving digital content. Some well-known online versions include:

- ▪ Digital Preservation Tutorial and Survey of Institutional Readiness from Cornell University.
- ▪ Digital Imaging Tutorial from LYRASIS.

A valuable support for life-long learning is the National Library of Australia's PADI (Preserving Access to Digital Information) site that provides a valuable educational framework and signpost relating to digital preservation issues (PADI 2009).

In summary, more capacity building in the area of digital preservation is needed across the region. Training provides a pathway of skills and experience critical to monitoring the guards. Training can also equip future guards with the vision, critical thinking skills, and ability to deal with future 'troops of conquest'; to proactively select, intervene, and collaborate across boundaries in order to safeguard digital heritage in the long term.

Conclusion

So much has been achieved in developing technological, organizational and resourcing strategies that mitigate the risks to digital content over a period of time. Applied in combination and with variation in approaches, they can potentially be a powerful defence against the dangers of digital destruction.

Notwithstanding these achievements, right now the risks in digital preservation still remains high, and the likelihood and consequences of loss are still dire – because these strategies are still in the early stages of

development and testing (Hoorens and Rothernberg 2008; Shenton 2009).

Or, to use Veheul's words: 'Digital preservation is still under construction' (Verheul 2006, p. 69).

Nonetheless, as we continue to build our globally interlinked digital repositories, there are three interlinked and absolutely pivotal options, which is believed to have the capacity to profoundly influence the survival of digital knowledge into the future. These are:

- Collaboration and alliances
- Risk management, quality assurance auditing and certification
- Education and training

As Colin Webb from the National Library of Australia insightfully comments: 'An effective preservation role in the library of the future will require flexibility, willingness to change, proactively seeking a useful role that draws on the expertise and perspectives we already have, while developing whatever new expertise and perspectives will be needed. Willingness to listen, consult, learn, and to form alliances and partnerships will all be important' (Webb 2002).

'Another face, another stage' and the story continues through time. The above three options, in combination, and using a variety of strategies, will effectively provide a framework for preservation of digital knowledge for the future.

Applying risk management systems, they will equip stakeholders with the vision and skills to rigorously and objectively keep on re-assessing that quintessential question: Who Guards the Guards?

References

Abbott D. 2003
Overcoming the dangers of technological obsolescence: rescuing the BBC Domesday project
DigiCULT.Info: a newsletter on digital culture, **4**, August, pp. 7–10

Adelstein P Z. 2003
Preservation of electronic records: status of ISO standards'
In *Symposium* 2003: *Preservation of electronic records*: *New Knowledge and Decision Making*
Ottawa, 15–18 December 2003: preprints

Ashley–Smith J. 1999
Risk assessment for object conservation
Oxford, Butterworth-Heinemann

Brindley L J. 2000
Keynote address to the Preservation 2000 conference.
New Review of Academic Librarianship **6:** 125–137

Brown H and Fenton A. 2005
Time's pivotal point – preserving the past for the future now
In *International Newspaper Librarianship for the 21st Century,* edited by H Walravens
IFLA Newspapers section. International Newspapers Conference: Asia and the Pacific: Newspapers in the 21st Century
22–24 February. National Library of Australia. Berlin, Saur, pp. 63–72. Details available at <http://www.reference-global.com/doi/abs/10.1515/9783598440205.2.63>, last accessed on 12 April 2009

Brown K S. 2005
Knowledge [unpublished poem]
K S Brown 13 September 2005

Buckley R. 2008
JPEG 2000 – a practical digital preservation standard? DPC Technology Watch Series report 08-01, Digital Preservation Coalition. Details available at <http://www.dpconline.org/docs/reports/dpctw08-01.pdf>, last accessed on 12 April 2009

CCSDS (Consultative Committee for Space Data Systems). 2002
Reference Model for an Open Archival Information System, (ISO Standard 14721).
Details available at <www.ccsds.org/publications/archive/650x0b1.pdf> last accessed on 2 April 2009

CHIN (Canadian Heritage Information Network). 2009
Capture your collections - planning and implementing digitization projects [online tutorial] CHIN
Details available at <http://www.chin.gc.ca/English/Digital_Content/Capture_Collections/index.html>, last accessed on 2 April 2009

Cornell University Library. 2009
Digital Preservation Tutorial, Details available at <www.library.cornell.edu/iris/tutorial/dpm/>,
Digital Timeline, Details available at <http://www.library.cornell.edu/iris/tutorial/dpm/timeline/viewall.html>,
last accessed on 2 April 2009

CRL (Center for Research Libraries). 2009
CRL's Certification and Assessment of Portico and Hathi Trust
Details available at <http://www.crl.edu/content.asp?l1=13&l2=58&l3=181> last accessed on 12 April 2009

Cullen C. 2000
Authentication of digital objects: lessons from an historian's research
In CLIR (Council on Library and Information Resources)
Authenticity in a Digital Environment, Washington, CLIR pp. 1–7

Dale R. 2006
Certifying Digital Repositories: Development of the Audit Checklist [and summing up comments] in APSR [Australian Partnerships for Sustainable Repositories]. *Long term repositories: taking the shock out of the future* 31 August–1 September 2006. Details available at <www.apsr.edu.au/presentations/longterm.html>, last accessed on 12 April 2009
Canberra: APSR

Deegan M and Tanner S. 2002
In *The Digital Dark Ages*, Update May 2002
Details available at <www.cilip.org.uk/publications/updatemagazine/archive/archive2002/may/update0205b.htm> last accessed on 2 April 2009

DELNET
Details available at <http://www.delnet.nic.in> last accessed on 2 April 2009

DPC (Digital Preservation Coalition). 2002
Preservation Management of Digital Materials – the Handbook by N Beagrie and M Jones Digital Preservation Coalition, UK (and decision tree) Details available at <www.dpconline.org/graphics/handbook/.htll>

Gaur R. 2009
Barriers to access Indian cultural heritage: copyright, permission rights and ownership issues vis-à-vis IGNCA collections
In Proceedings Indo-US Workshop on international trends in digital preservation, March 24–25 2009, Human Centred Design and Computing, CDAC, Pune, India pp. 20–30. Details available at <http://www.ndpp.in/indo_us.html>, last accessed 15 July 2009.

Guenther R. 2006
The promise of PREMIS: background, scope and purpose of the 'Data Dictionary for Preservation Metadata' in APSR
[Australian Partnerships for Sustainable Repositories]
Long term repositories: taking the shock out of the future. 31 August–1 September 2006, Canberra, APSR
Details available at <http://www.apsr.edu.au/presentations/longterm.html>, last accessed on 12 April 2009

Harvey R. 2005
Preserving Digital Materials
Munchen: K G Saur

HATII (the Humanities Advanced Technology and Information Institute) at the University of Glasgow
Details available at <http://www.hatii.arts.gla.ac.uk>, last accessed on 2 April 2009

Hoorens S and Rothernberg J. 2008
Digital preservation: the uncertain future of saving the past RAND Project resource, RAND Europe
Details available at <http://www.rand.org/pubs/research_briefs/RB9331/> last accessed on 12 April 2009

Hunter J. 2006
Putting the shock back into the future
In APSR [Australian Partnerships for Sustainable Repositories]
Long term repositories: taking the shock out of the future 31 August–1 September 2006, Canberra, APSR
Details available at <http://www.apsr.edu.au/presentations/longterm.html., last accessed on 12 April 2009

ICDL (International Conference on Digital Libraries). 2006
Details available at <http://www.teriin.org/events/icdl/> last accessed 12 April 2009
New Delhi: The Energy and Resources Institute

IFLA Newspapers section
- 1996, *Guidelines for Newspaper Preservation Microfilming*
- 2002, Microfilming for Digitisation and Optical Character Recognition: Supplement to Guidelines
Details available at <http://www.ifla.org/VII/s39/broch/microfilming.htm>, last accessed on 12 April 2009

IGNCA (Indira Gandhi National Centre for the Arts). 2009
Seminar on Digital Preservation and Access to Indian Cultural Heritage with special reference to IGNCA Cultural
Knowledge Resources 31 January–1 February 2009
Details available at <http://ignca.nic.in/kn_digital_program.htm>

National Archives of Singapore. 2009
Details available at <http://www.nhb.gov.sg> last accessed on 12 April 2009

National Library of Australia
- Web Archiving Conference November 2004
  Details available at <http://www.nla.gov.au/>, last accessed on 2 April 2009

- Australian Newspapers Digitisation Program. 2007 National Library of Australia Persistent Identification Model for
  Newspapers
  Details available at <http://www.nla.gov.au/ndp/project_details/documents/ANDP_Newspaper_PIs_v1.0p>

- Digital Preservation Policy 2008 (3rd ed)
  Details available at <http://www.nla.gov.au/policy/digpres.html> last accessed on 2 April 2009

NNM (National Mission for Manuscripts [India]). 2009
Details available at <http://namami.org/index.htm> last accessed on 2 April 2009

NESTOR. 2006
Details available at <http://www.langzeitarchivierung.de/> last accessed on 12 April 2009

Nestor Working Group on Trusted Repositories Certification. June 2006
Catalogue of Criteria for Trusted Digital Repositories. Version 1 (draft for public comment)
English translation December 2006. urn:nbn:de:0008-2006060703.
edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf

NSF-DELOS Working Group on Digital Archiving and Preservation. 2003
Invest to save: report and recommendations of the NSF-DELOS Working Group on Digital Archiving and Preservation
National Science Foundation and the European Union

OCLC and Research Libraries Group (RLG). 2002
Trusted Digital Repositories: Attributes and Responsibilities
Details available at <http://www.oclc.org/au/en/digitalpreservation/resources/default.htm> last accessed on 2 April 2009

PADI (Preserving Access to Digital information). 2009
Details available at <http://www.nla.gov.au/padi/> last accessed on 2 April 2009

Palm J. 2006
The digital black hole
[Jonas Palm, Director, Head of Department of Preservation, Riksarvet/National Archives, Stockholm Sweden – article posted May 2006]
Details available at <http://www.tape-online.net/docs/Palm_Black-Hole.pdf> last accessed on 14 June 2006
The article is published in the framework of the TAPE project: Training for Audiovisual Preservation in Europe, <http://www.tape-online.net/>

Pandora
Details available at <http://www.nla.gov.au/pandora/> last accessed on 2 April 2009

Phillips M. 2002
Archiving the web: the National Collection of Australian Online Publications
Paper presented at the International Symposium on Web Archiving, National Diet Library, Tokyo, Japan 2002.
Details available at <http://www.nla.gov.au/nla/staff-paper/2002/phillips1.html> last accessed on 2 April 2009

PLANETS (Preservation and Long-term Access through Networked Services). 2009
Details available at <http://www.planets-project.eu/> last accessed on 2 April 2009

Rassmussen E and Choi Youngok. 2006
Digital librarians for digital libraries
In *ICDL International Conference on Digital Libraries*,
New Delhi: TERI. pp. 748–754

Shenton H. 2009
Digital versus print as a preservation format – Expert views from international comparator libraries
Details available at <http://www.bl.uk/aboutus/stratpolprog/ccare/introduction/digital/digitalvprint/index.html>,
last accessed on 12 April 2009

Smith A. 2003
New-model scholarship – how will it survive?
Washington, DC: Council on Library and Information Resources

Smith A. 2004
The future of web resources: who decides what gets saved and how do they do it
Paper delivered at international conference Archiving Web Resources: issues for cultural heritage institutions
9–11 November 2004
Canberra: National Library of Australia

Smith B. 2002
Preserving tomorrow's memory: preserving digital content for future generations
Information Services & Use, **22**: pp. 133–139

SOLINET Digital Imaging Tutorial
Details available at <http://www.solinet.net/workshops/workshop_templ.cfm?doc_id=1085> last accessed on 13 April 2009

State Library of South Australia
Details available at <http://www.slsa.sa.gov.au> last accessed on 13 April 2009

UNESCO. 2003
Guidelines for the Preservation of Digital Heritage, prepared by the National Library of Australia
Paris: UNESCO.
Details available at <http://www.unesdoc.unesco.org/images/0013/001300/13007le.pdf> last accessed on 13 April 2009

UNESCO. 2004
Charter on the Preservation of Digital Heritage
Paris: UNESCO
Details available at <http://www.unesco.org.ci/en/file_download.php/4cc126a2692a22c7c7dcc5ef2e2878c7Charter_en.pdf>,
last accessed on 13 April 2009

University of South Australia. 2009
Business and Information Management course
Details available at <http://www.unisa.edu.au/bim/> last accessed on 12 April 2009

US-Inter PARES Project. 2002
InterPARES Interpreted: a guide to findings on the preservation of authentic electronic record
Details available at <http://www.gseis.ucla.edu/us-interpares/pdf/InterPARESInterpreted.pdf>, last accessed on 12 April 2009

Verheul I. 2006
Networking for Digital Preservation: Current Practice in 15 National Libraries (IFLA Publications 119)
Munchen: K G Saur.

Webb C. 2004
The malleability of fire: preserving digital information
In *Managing preservation for Libraries and archives: current practice and future developments*, edited by Feather, J Ashgate,
Aldershot. pp. 27–52

Woodyard-Robinson D. 2006
Common use cases for preservation metadata
In APSR [Australian Partnerships for Sustainable Repositories]
Long term repositories: taking the shock out of the future, 31 August–1 September 2006
Canberra: APSR
Details available at <http://www.apsr.edu.au/presentations/longterm.html>, last accessed on 12 April 2009

Bibliography

Adams D, *et. al.* 2004
**Addressing a risk perspective when considering digitisation as a preservation reformatting method: a response from
'down under'**
Microform and Imaging Review **33**(4): Autumn pp. 188–189

Arthur K, *et al.* 2004
Recognizing Digitization as a Preservation Reformatting Method
Prepared for the ARL Preservation of Research Library Materials Committee
Details available at <http://www.arl.org/preserv/digit_final.html> last accessed on 2 April 2009

Beagrie N. 2004
The Continuing Access and Digital Preservation Strategy for the UK Joint Information Systems Committee
In *D-Lib magazine*, **10**(7/8) July. Details available at <http://www.dlib.org/dlib/july04/beagrie/07beagrie.html>
last accessed on 2 April 2009

British Library. 2007
British Library Digital Preservation Strategy
Details available at <http://www.bl.uk/aboutus/stratpolprog/ccare/introduction/digital/digpresstrat.pdf>

De Lusenet, Yola 2007
Tending the garden or harvesting the fields: digital preservation and the UNESCO Charter on the Preservation of Digital heritage
In *Library Trends Summer* **56**(1). pp.164–182

DRAMBORA (The Digital Repository Audit Method Based on Risk Assessment)
The Digital Repository Audit Method Based on Risk Assessment 2009
Details available at <http://www.repositoryaudit.eu/> last accessed on 12 April 2009

Harvey R. 1993
Preservation in Australian and New Zealand Libraries: principles, strategies and practice for librarians, 2nd ed
Wagga Wagga, Centre for Information Studies, Charles Sturt University

Hedstrom M. 1998
Digital preservation: a time bomb for digital libraries
In *Computers and Humanities,* **31**: pp. 189–202

Hodge G and Frangakis E. 2004
Digital preservation and permanent access to scientific information: the state of the practice
A report sponsored by the International Council for Scientific and Technical Information (ICSTI) and CEDNI
Details available at <http://cendi.dtic.mil/publications/04-3dig_preserv.html>, last accessed on 13 April 2009

ICADS [a joint alliance of IFLA and the Conference of Directors of National Libraries]
Details available at <http://www.nla.gov.au/padi/topics/712.html> last accessed on 9 April 2009

The Internet Archive
Details available at <http://www.archive.org>, last accessed on 2 April 2009

I**nternational Internet Preservation Consortium**
Details available at <http://www.netpreserv.org> last accessed on 2 April 2009.

JISC (Joint Information Systems Committee). 2009
Digital Preservation Training Program
Details available at <http://www.ulcc.ac.uk/dptp/> last accessed on 2 April 2009

Kenney A, *et al.* 2006
E-Journal Archiving Metes and Bounds: A Survey of the Landscape
CLIR pub 138, CLIR September, 2006
Details available at <http://www.clir.org/PUBS/reports/pub138/pub138.pdf> last accessed on 12 April 2009

LYRASIS (formerly SOLINET) Distance Education courses. Digital Imaging of Library and Archival Materials
http://www.lyrasis.org/Classes-and-Events/Tracks/Digitization.aspx last accessed on 12 July 2009