Failure as process: interrogating disaster, loss, and recovery in digital preservation

Carly Dearborn
Sam Meister

Abstract

Disaster, loss, and failure preoccupy the minds of many digital preservation professionals and yet, despite the prominence of digital disaster planning guidelines which seem to anticipate failure, there is limited discussion of experience with preservation system or network failures, which are often framed as inevitable in digital preservation. Despite this framing, negative perceptions of failure influence the digital preservation discourse by associating failure with poor planning, unreliability, and untrustworthiness on the part of institutions. This article will interrogate the issue of failure within the digital preservation field and consider the need for more conversations around network failure and recovery. The authors will argue that failure is part of the process of digital preservation and more honest conversations around this topic will contribute to the practice of openness and transparency within the digital preservation community. To illustrate these issues the authors will discuss the actual hardware failures experienced by the MetaArchive Cooperative, a community-based distributed digital preservation network, and how the Cooperative's utilization of the LOCKSS software allowed it to recover from those failures. Additionally, the lessons learned and resulting changes the Cooperative made to technical infrastructure, hardware diversity, policies and procedures will be shared.

Keywords

Digital preservation, Failure, Distributed digital preservation, High reliability organizations, Transparency

Introduction

Digital preservation is a risky endeavor. The nature and variety of threats to digital content necessitate a multiplicity of strategies and constant vigilance on the part of practitioners and organizations responsible for ensuring ongoing preservation and access. These threats come in many shapes and sizes, from microscopic bit-level corruption, to accidental deletion by human error, to catastrophic damage from natural disasters.

Threats to digital content also occur at different speeds, from hard drive crashes happening suddenly and dramatically, to file format obsolescence that may come about at more gradual pace.

Loss of digital content is inevitable, whether due to never being captured and acquired into digital preservation systems, or loss that occurs during management within those systems. While it is difficult to measure how much digital content is not being captured, there is some potential for understanding the nature and degree of loss and/or failure that is happening within the systems that are controlled and managed. Even though this potential exists, there is currently limited knowledge about digital preservation failures because accounts of failure and loss are rarely shared openly or with much useful detail. Most digital preservation strategies are designed to mitigate against a range of risks and threats, but this mitigation often includes an acceptable degree of loss depending on the complexity of the digital objects being preserved. Risk assessment efforts and disaster recovery planning initiatives have encouraged institutions to think about failure strategically and to develop responses to identified risks or potential failure points. This article builds on risk management principles and approaches digital preservation and risk management as one and the same.

This article will interrogate the issue of failure within the digital preservation community. It will first explore what failure means within this community, how it has evolved, is anticipated, and measured. Borrowing from organizational psychology, the authors argue that the digital preservation field should adopt a mindset of doubt and practice a *preoccupation with failure* in order to first understand why failures occur and then to prevent them. The principles governing high reliability organizations (HROs), or organizations where despite the high risk of their activities experience few accidents, provide a useful framework to consider how open discussions around points of failure can benefit the digital preservation field at large. The authors argue that the digital preservation field should not see success and failure as opposites on a spectrum but rather that failure can inform work towards success. To illustrate this point, the final section of this article will include a discussion of the past failures experienced by the MetaArchive Cooperative, a community-based distributed digital preservation network. It is the authors' hope that this discussion will open opportunities for others to share similar stories and encourage a field-wide preoccupation with failure that may benefit all practitioners and institutions preserving digital assets over the long-term.

Interrogating Failure

The language used to describe digital preservation practices, theories and policies implies that some degree of failure is inevitable. From the absence of absolute terms like *permanent* or *forever*, to the measured language describing outcomes of major preservation strategies such as migration or emulation, conversations about digital preservation goals and capabilities are typically pragmatic and restrained. This approach borrows heavily from language used in the archives field. O'Toole (1989) traces the quest for documentary permanence throughout archival history, ultimately arriving at the point where archivists and records managers, when faced with the ever-increasing size of physical materials needing conservation treatment, realized that the goal of permanence was unattainable and perhaps impossible. Coupled with the realization that the very concept of permanence undermined appraisal efforts, archivists stopped speaking in terms of permanence. In the 1980s the Society of American Archivists (SAA) abandoned phrases such as *permanent records* in favor of *records of enduring value*, thus deserting the very idea of absolute archival permanence (O'Toole, 1989: 23). The digital preservation community, aware of how quickly technology advances and how storage costs decrease, also avoids language which appears to guarantee certain outcomes or access. In fact, some institutional policies explicitly state that perpetual access cannot be guaranteed long term (Dartmouth, 2015) or may only commit to preserve certain properties of a digital object (i.e. intellectual content over interoperability). To call these attempts to manage expectations an admittance of failure would be unfair -- rather, they represent a willingness on the part of those in the digital preservation community to speak realistically about the challenges of preserving digital objects.

Open discussions and communication on the topic of failure lead naturally to failure's perceived opposite: success. Success in digital preservation is difficult to measure. For one, the field is still relatively young. Despite pockets of consensus around the need to preserve digital records in the 1960s (when ICPSRs' data archive was established), concerted effort to preserve digital records largely emerged in the 1980s and 1990s alongside advances in personal computing (Digital Preservation Management, 2013). Now, as many institutions enter the third decade of actively maintaining and preserving digital records, initiatives focusing on the assessment of digital preservation activities are becoming more regularly visible. While this is indicative of a maturing field, true assessment is difficult without agreed upon definitions of success. Based on experience and work to date, there is some consensus in the field on the requirements of successful digital preservation activities. Barateiro, et al. (2010) outlined many of these requirements, which include reliability, authenticity, provenance, integrity, measures to combat obsolescence, scalability, and heterogeneity. These requirements, in one version or another, inform the bulk of preservation strategies as outlined in institutional policies. It is important to note, however, that it is difficult to clearly define all the requirements as each institution's needs will vary depending on type and amount of digital records and the specific goals of each institution.

Further complicating the definition of success, there is not always a definite point in time when it becomes obvious that an initiative or action is successful. Success in digital preservation will likely be measured at some vague end point by the absence of certain events: the absence of format obsolescence, the absence of bit rot, the absence of a server failure. This timescale is at odds with contemporary notions of success. A startup business can be successful in its third quarter, a marketing campaign over the course of a year, a political candidate on election day. Distributed digital preservation, which will be discussed later in this article, is considered to have become one of the successful strategies of the past ten years -- but in preservation, past metrics of measurement can quickly become out of date. Success in digital preservation will always be a moving target. Shifting the focus of digital preservation dialogue away from success and towards understanding of past failures and anticipation of future points of failure is a more productive endeavor.

There are models from other fields and industries that could assist in reframing the concept of failure for digital preservation. Social psychologists Weick and Sutcliffe discuss the resiliency of high reliability organizations (HROs) by crediting an organizational culture of attention to indications of failure, simplification, operations, resilience, and expertise (2015: 7). HROs are organizations that, despite daily operations high in risk and complexity, have a relatively low failure and accident rate (Weick and Sutcliffe, 2015: 2). Examples of HROs include aircraft carriers, nuclear power operations, or emergency response services. While risks such as loss of life or nuclear accident are not the same kind of risks faced by cultural heritage institutions, the lessons and culture of HROs can translate to organizations where the potential risks take the form of threats to cultural heritage assets, credibility, trust, and public goodwill.

HRO's share five principles of operation: a preoccupation with failure, a reluctance to accept simplifications, sensitivity to operations, commitment to resilience, and a deference to expertise. For the purpose of this article, special focus will be paid to the first principle. Preoccupation with failure represents an organization's attention to the small cues and anomalies which could be symptomatic of a larger failure event. When organizations only value and pay attention to positive results, the seemingly insignificant disruptions go unnoticed until it might be too late. Focusing on only positive events, results, or news is not only misleading to the real development and processes occurring behind the scenes but it can support unrealistic or inaccurate norms. In psychology and other behavioral sciences, focus on the positive or statistically significant studies result in what is referred to as the "file drawer problem," or the publication bias that occurs when journals only publish statistically significant results and relegate to the file drawer those with non-significant results (Rosenthal, 1979). The absence of nonconforming results from the literature has the potential to create a bias in meta-analysis and distort the collective research of the field to support or oppose a particular point of view (Pautasso, 2010). To avoid a digital preservation version of “file drawer problem” and support a culture where anomalies are noticed, discussed, and not normalized, the field should learn from HROs to view even small instances of failure as instructive to the entire community. Failure is not inherently opposed to success - intentionally and critically engaging with failure can lead to success.

A preoccupation with failure also recognizes that the knowledge of a group or organization is often incomplete, especially in circumstances with changing environments or unfamiliar tasks and problems. Weick and Sutcliffe discuss cultivating a mindset of doubt as a critical step in recognizing limits to existing knowledge and therefore, in managing the unexpected (2015: 52). They point to a fellow organizational psychologist (Kramer, 2007: 17) who states that “if the environment is dynamically complex it is impossible to know and understand everything in advance therefore you need to be able to doubt your existing insights”. Doubt allows room for critical questioning of existing knowledge and can create space for anomalies or cues of failure to be identified and more quickly dealt with. Digital preservation practitioners frequently meet the limits of their own or the field's collective knowledge due to changing technology and diversity of formats and structures in digital collections.

The ability to use doubt to the benefit and safety of an organization comes with being able to organize and structure discussions around problems without clear solutions. This can be achieved through an institutional "spirit of contradiction" or an encouragement of alternative views, controversy, and criticism (Weick and Sutcliffe, 2015: 52). In a similar vein, Halberstam (2011) explores alternative definitions and experiences of success in a "traditionally" cisgender, heteronormative, capitalist world, introducing low theory as alternative, counterintuitive modes of knowing, learning and existing. Halberstam argues that in the "traditionally" negative spaces of critique, confrontation and failure are where creativity, innovation, and experimentation can thrive (2011: 10). While this spirit of contradiction and evidence of low theory can be found informally at digital preservation conferences and meetups, it is important that the digital preservation field continues to foster and expand these conversations and does not avoid controversy and presentations of unresolved failure in favor of neat, tidy, positive, and successful projects.

Failure, doubt, and disappointment are not unfamiliar to those working in digital preservation. Practitioners often deal exclusively in peculiar situations with collections diverse in format and complexity. The digital preservation field, faced with the challenge of preserving digital objects through unexpected and unforeseeable challenges, depends on a spirit of sharing, collaboration, experimentation, and perhaps most importantly transparency. Practitioners use and create open source tools and programs, found collaborative organizations which utilize cost sharing, and recommend the adoption of open and well-documented formats. Despite a field-wide focus and encouragement of openness and transparency, there is still a very human tendency to withhold examples of failure or data loss in fear of a threat to reputation or trustworthiness. This lack of transparency poses a risk to the whole community which could benefit from open discussion and understanding of failure events (Rosenthal, et al. 2005). The potential of damaged personal or institutional reputation is a very real outcome of sharing accounts of failure, and points to the need for additional public communication channels to safely share failure details. An online space where individuals could share anonymized information about failures could be one kind of strategy, but the limited details about failure events related to such anonymity would need to be weighed against the value to the larger community. The authors recognize concern over reputation damage as a barrier to sharing failures, and do not presume to have a solution, but instead encourage continued community dialogue and debate on this issue.

The recognition of the need to share mistakes, failures and stories of data loss has not gone unnoticed in the digital preservation community. There have been initiatives which called attention to this issue, although, none have received field-wide traction or support. Barbara Sierman, the Digital Preservation Manager at the national Library of the Netherlands raised the issue of documenting digital preservation failures on her Digital Preservation Seeds blog in 2012 (Sierman). The post gained immediate interest and as a result, Sierman created a Flickr group devoted to the photographic documentation of digital damages, errors, and failures in preservation activities as well as the Atlas of Digital Damages blog and website that includes references to articles detailing events of data loss or digital decay. Recently, the Society for American Archivists Electronic Records Section blog released a call for contributions specifically dealing with digital preservation failures and the lessons learned from them (SAA ERS, 2017). This new initiative to encourage open discussions of digital preservation failure is an exciting step and the authors hope it represents a change in both scholarship and practical applications of digital preservation.

Both these efforts are admirable; however, they are unsustainable if only managed by one person or even one organization. The digital preservation field as a whole needs to approach failure or data loss as part of the process of preservation. The field needs general acceptance that discussing, presenting, and publishing on errors, failure, or loss will benefit the greater good and build a community of knowledge sharing that all practitioners can learn from. It means not glossing over embarrassing failures and focusing too much on successful anomalies which cannot be reproduced. If the digital preservation community does not address and bring attention to the small errors, challenges, failures, and losses experienced individually, it will be less prepared as a field to address the larger more complicated challenges that are sure to come.

The emergence in some fields of journals of negative results combats the “file drawer problem” and encourages the idea that positive or statistically significant results are not the only research worth publishing and sharing. *The Journal of Negative Results in Biomedicine*, an open access, peer-reviewed journal founded in 2002 provides a platform for scientists in biomedicine to publish negative, "unexpected, controversial and provocative" results (Journal of Negative Results in BioMedicine). Similar journals exist in physics, ecology, nanotechnology, and other fields. Professionals in wildland management can contribute to the Wildland Fire Lessons Learned Center, an interagency database containing incident reviews and reports from around the country. These examples illustrate that the necessity to explore and learn from failures is a universal concern in all areas of academia and beyond.

As an attempt to provide an example of sharing stories of failure in digital preservation, two episodes of failure that have occurred within the MetaArchive Cooperative are outlined below. The intention in recounting the details of these technical failures is to illustrate that each of these episodes in turn motivated specific changes within the MetaArchive technical infrastructure and policies, resulting in a stronger and more secure digital preservation network. In many ways, these "growing pains" have demonstrated the value of both the Lots Of Copies Keep Stuff Safe (LOCKSS) technical approach to distributed digital preservation, as well as the underlying MetaArchive philosophy and organizational approach of embedding digital preservation knowledge and activities within institutions. MetaArchive community members understand that some level of technical or human failure is bound to occur, but see this as part of the process of doing digital preservation, being able to evolve and shift strategies as a results of lessons learned from failure events.

MetaArchive Cooperative: Failure and change

The MetaArchive Cooperative was founded on the premise that by actively engaging in community-based collaboration, cultural heritage institutions can best position themselves to overcome the challenges of preserving digital information over the long-term. Utilizing a network-based distributed digital preservation approach that replicates copies of digital collections geographically, MetaArchive Cooperative members collaborate to preserve each other's digital content, achieving fundamental bit-level digital preservation and protecting against a range of natural and man-made risks. Since its founding in 2004, the MetaArchive Cooperative has encountered multiple risk scenarios at both the institutional and network-wide level, and has recovered digital content without catastrophic loss.

As a Private LOCKSS Network (PLN), the MetaArchive Cooperative utilizes a specialized application of the LOCKSS protocol and function, using the same software as the public Global LOCKSS network. While the Global LOCKSS network focuses on the preservation of electronic journals, MetaArchive is format agnostic, and has preserved a wide variety of content including newspapers, electronic theses and dissertations, photographs, audio, video, and datasets.

As the Cooperative transitioned from a Library of Congress funded research project to a membership organization in 2007, it continued the community-owned and operated philosophy in the establishment of its governance structure. MetaArchive is an affiliated community of the Educopia Institute, which provides administrative, fiscal, and legal support, but it is governed and led by a Steering Committee and elected leadership group which reviews and sets policies and procedures for all aspects of the organization. This member-led, member-driven nature of the organizational structure has motivated a culture of transparency in relation to both high level policy decisions, such as membership fees, as well as technical network operations, including reporting on multiple incidents of technical failure that have occurred over the years.

Episode 1: A Bunch of Power Failures

The first failure event occurred in November 2007, during the early days of the MetaArchive transition from a Library of Congress funded research project to an independent membership organization. While conducting a series of disaster recovery tests to evaluate overall network operations and performance an actual, unplanned, failure took place at Emory University, one of the network's primary storage nodes at that time. The event started with an initial power failure that affected the uninterruptable power supplies (UPS) servicing both the server hosting the LOCKSS software and the storage array attached to the server. The cause of the issue appeared to be that the UPS had been connected to two power outlets on a single circuit, rather than two separate circuits. A work order was placed to resolve the issue, and the UPS was moved to the remaining unoccupied power circuit so that the critical systems could be examined to determine any damage. A cursory filesystem check revealed that multiple virtual disks had experienced some level of corruption. Repairs to damaged filesystems were initiated, with an expectation of completing in 8-12 hours. After this first round of repairs completed, additional damage was discovered during a more detailed examination, and a second round of repairs was initiated.

As if on cue, the sole remaining circuit powering the UPS failed during this additional filesystem repair session. An escalated call to facilities led to power being quickly restored and the UPS was connected to separate power circuits. Once the server and storage array were back online, the storage array reported a new failure of two disks, compromising the RAID 5 configuration which can can only withstand the loss of a single disk before irreparable corruption occurs. Happily, a second test of the system, resulted in the reporting of only a single disk failure, which allowed for the replacing of the failed disk and the rebuilding of the RAID. Even with the successful RAID rebuild, it was determined that the damaged filesystems were beyond recovery and needed to reformatted and the data restored from other network storage nodes. This process was initiated and the data was successfully restored in a matter of hours.

The results of this unplanned failure event included both a confirmation of the robustness of the LOCKSS network approach as well as recommendations for procedures to follow for future disaster event scenarios. The corruption of filesystems housing data or the failure of the storage media containing those filesystems that occurred during the described event is among the most likely recoverable failures of any LOCKSS node. Even though the attempts to recover the filesystem were delayed by a second power failure, the process consumed a great deal of time, and these filesystems were likely beyond recovery even before the second failure occurred. Checking and repairing three large filesystems took far more time than the later solution of simply reformatting the disks and re-crawling the data from remote sources. An unanticipated lesson of the episode was that even less significant hardware or filesystem failures are sometimes more easily recovered from remote sources. Although the LOCKSS system provides for the automatic detection and repair of corrupted data, this episode resulted in the recommendation to recover damaged filesystems from other machines in a network rather than by attempting filesystem repairs to limit the overall downtime for storage nodes.

Episode 2: Different is better

Another significant failure event occurred during 2011-2012 and was related to an early implementation of the MetaArchive hardware refresh policy. The policy outlined that server hardware were to be refreshed and replaced on a three-year cycle to mitigate against technological obsolescence and inevitable disk failures. This hardware refresh policy was connected to set of technical specifications that outlined the details of hardware and software requirements needed to setup and configure a storage node in the network. In the early period of the MetaArchive network, these specifications included recommended hardware vendors and models that supported these requirements. Most members selected the recommended hardware vendor and as a result, the first three generations of storage nodes in the technical network infrastructure all utilized a similar hardware vendor for each generation. By 2011, server hardware from the second generation vendor, Capricorn Technologies, was due for retirement and transition to third generation hardware from Iron Systems. This refresh process included the secure migration of data utilizing rsync and a set of custom scripts. Unfortunately, during the process of migrating collection content from the Capricorn servers to the Iron Systems servers, numerous Iron Systems destination servers experienced an immediate series of disk failures. After extensive evaluation, the reasons for this tidal wave of disk failures could not be attributed to any specific software vulnerability and were likely due to manufacturing weaknesses.

As with the previous power failure scenario, the ability to restore local copies of data lost due to disk failures from other copies in the private LOCKSS network mitigated against the potential for unrecoverable data loss. In fact, this failure episode emphasized the value of the default LOCKSS approach of having seven copies of data stored at seven different geographically distributed locations. Even with multiple hardware failures occurring at relatively the same time across multiple nodes in the network, there was no point during this period where any collection content had less than three distributed copies. Plus, this higher number of copies ensured that there would be sufficient copies at nodes where disk failures had not been experienced to restore from.

Equally important, this experience of cascading disk failures from a single hardware vendor highlighted the need for a different approach in relation to the technical specifications. As a result, the MetaArchive technical specifications no longer include recommendations for specific single hardware vendors, but instead a range of vendors and models are encouraged that can support the minimum requirements. This has resulted in more heterogeneous technical network infrastructure in relation to both hardware vendors and refresh cycles.

Each of the above failure episodes are situated in the context of the early stages of development of an organization building the foundation of a distributed digital preservation network. In this scenario the potential for mistakes and failures is high as new technical strategies and approaches are implemented, but this is not the only period in which monitoring, critical evaluation, and discussion of failures is important. Interpreting these two episodes as successful is a convenient narrative; however, it is important for the MetaArchive Cooperative and the larger digital preservation community to also see the danger in the close calls rather than the just success. Interpreting a close call as successful can contribute to beliefs that current workflows are adequate deterrence to failure and not in need of improvement (Weick and Sutcliffe, 2015: 10). For organizations with digital preservation responsibilities this is an ongoing endeavor, one that entails dedicated focus and resource allocation. In the case of the MetaArchive Cooperative, the organizational culture and structures of communication and transparency provided a framework to openly share the details of each failure event across the entire membership so that collectively a resolution and shifting of strategies could be enacted with member-wide input. It should also be noted that this is not the first time that MetaArchive failure events have been publicly shared, as community members have previously presented and published (Halbert and Trehub, 2012) on this topic in an effort to engage the larger digital preservation community. While the failure events described occurred within a network of organizations, there is clearly potential for a similar mode of sharing, learning, and growth to be implemented across the digital preservation field.

Conclusion

The digital preservation field has a complicated relationship with the concept of failure. While expecting a certain degree of failure, it measures success by a lack of failure. While encouraging openness and transparency, it avoids critical and detailed discussions of loss or failure events. By adopting the mindset and principles of high reliability organizations, the digital preservation field can engage critically with past failures, build collective knowledge of how failure can occur, and anticipate or develop a sensitivity to future failures. Seeing failure as part of the process of digital preservation, one that should be studied, discussed, and remembered, is crucial to the success of organizations, initiatives, and projects. The discussion of MetaArchive Cooperative's past technical failures and subsequent adjustments to infrastructure and organizational capabilities hopefully demonstrates a first step towards cultivating a preoccupation with failure in the digital preservation community. Simply publishing these accounts may not be enough, but it is a start. To further this effort, the digital preservation field needs to continue to support a spirit of contradiction, see the value in pessimism and doubt, and encourage the investigation of alternative solutions.

References

Barateiro J, Antunes G, Freitas F, and Borbimha J (2010) Designing Digital Preservation Solutions: A Risk Management-Based Approach. *International Journal of Digital Curation* 5(1):4-17.

Dartmouth College Library (2015) Digital Preservation Policy. Available at https://www.dartmouth.edu/~library/preservation/docs/dartmouth_digital_preservation_policy.pdf

Digital Preservation Management (2013) Timeline: Digital Technology and Preservation. Available at: http://www.dpworkshop.org/dpm-eng/timeline/viewall.html (Accessed 2 Feb. 2017)

Halberstam, J (2011) *The Queer Art Of Failure*. Durham NC: Duke University Press.

Halbert M and Trehub A (2012) Safety in Numbers: Distributed Digital Preservation Networks. In: *78th IFLA General Conference and Assembly Proceedings*, Helsinki, Finland, 11-17 August 2012.

Journal of Negative Results in BioMedicine (2017) About. Available at: https://jnrbm.biomedcentral.com/about (accessed 18 Feb. 2017)

Kramer, EH (2014) *Organizing Doubt: Grounded Theory, Army Units and Dealing with Dynamic Complexity*. Frederiksberg: Samfundslitteratur.

LOCKSS (2017) What is LOCKSS? Available at: https://www.lockss.org/about/what-is-lockss/ (accessed 31 Mar. 2017)

O'Toole, (1989) On The Idea Of Permanence. *The American Archivis*t 52(1): 10-25.

Pautasso, M (2010) Worsening File-Drawer Problem In The Abstracts Of Natural, Medical And Social Science Databases. *Scientometrics* 85(1): 193-202.

Rosenthal DSH, Robertson T, Lipkis T, Reich V, and Morabito S (2005) Requirements For Digital Preservation Systems. *D-Lib Magazine* 11.11: n. pag.

Rosenthal, R (1979) The File Drawer Problem And Tolerance For Null Results. *Psychological Bulletin* 86(3): 638-641.

SAA bloggERS! (2017) Call For Contributors – #Digitalarchivesfail: A Celebration Of Failure Web. Available at: https://saaers.wordpress.com/2017/01/10/call-for-contributors-digitalarchivesfail-a-celebration-of-failure/comment-page-1/ (accessed 18 Feb. 2017)

Sierman, B (2015) Atlas of Digital Damages. Available at: http://www.atlasofdigitaldamages.info/ (accessed 2 Feb. 2017)

Weick KE, and Sutcliffe KM (2015) M*anaging The Unexpected: Sustained Performance In A Complex World*. Hoboken, New Jersey: John Wiley & Sons.

Wildland Fire Lessons Learned Center. (2017) Home. Available at: Wildfirelessons.net (accessed 22 Feb. 2017)