1-1-2015

The University of Iowa and the Flood of 2008: A Case Study

Paul A Soderdahl
University of Iowa

Mallery, Mary. 2015. *Technology disaster response and recovery planning: a LITA guide*.

Case Study: University of Iowa and the Flood of 2008

Paul A. Soderdahl

Introduction

> *Tuesday, May 28, 2013. "The University of Iowa is taking a number of precautionary measures to prepare for potential flooding as the area copes with prolonged rainfall. A media briefing is scheduled for 4:30 p.m. Tuesday."*

Nearly five years after the devastating flood of 2008, university officials mobilized the critical incident management team and dusted off the flood emergency response plan, a now-familiar supplement to the university's overall critical incident management plan. Back in the summer of 1993, the emergency spillway at the Coralville Dam, nine miles upstream from campus, was breached for the first time. The University of Iowa, having suffered $6 million in damages from this "100-year flood," developed a response plan to guide emergency decision-making in future floods.[1]

Fifteen years later in the summer of 2008, the spillway was breached again. University officials followed the flood response plan, but the Iowa River rose to unprecedented levels never contemplated in the original plan. This "500-year flood" came at an exponentially greater cost of $743 million.[2] Capital improvements were made throughout campus to mitigate against future flood damage, and the flood response plan was significantly updated.

The revised plan was finalized in 2012, just in time to guide the coordinated response when the river quickly rose the following May. On Tuesday, the day after Memorial Day, the water was high enough to trigger the first set of action items for the main library and several

other campus buildings. By Thursday, efforts were underway to remove books from the lowest shelves. On Friday, the art library – located on the opposite banks of the river – was shuttered because the new removable flood wall, engineered after the 2008 flood, blocked all access to and from the building. Experts predicted the spillway would be breached a third time. Fortunately, several days of unexpectedly dry weather soon followed and the river, though still well above flood stage, caused little damage to university property.

For library IT staff, the devastating 2008 flood was an unwelcome test of a 4-month-old library IT disaster response plan. Five years later, the 2013 scare offered an opportunity to see if the lessons learned from 2008 were on point.

This case study will detail the long process involved in drafting the library IT disaster response plan, details of how the plan was executed during the flood of 2008, new strategies to mitigate risk, lessons learned in 2008, and observations from 2013.

Drafting the Plan

Every organization recognizes the need for an IT disaster response plan – one that articulates priorities, enables quick decision-making during a crisis, details requirements for continuity of service, and guides recovery efforts. Trying to put pen to paper, however, is a daunting task.

Outside of the IT realm, a typical library has endured decades of small and large crises that impact library operations and put for the physical collections at risk. Libraries have created whole departments around “continuity of service” (circulation) and “risk mitigation” (preservation). It is no wonder, then, that libraries typically have mature plans at the ready for crises affecting the physical collection. By comparison, a library IT disaster response plan is a nascent document.

The university's enterprise-wide IT disaster plan published in 2004 was more of a call to action rather than a plan of action. The documented stated that "each unit must produce and maintain a Disaster Recovery Plan in order to be prepared to continue doing business in the event of a severe disruption or disaster. The focus of the plan is on actions needed to restore services and necessary operations in the event of a loss of critical functions."

In early 2005, a library task force was charged to develop a departmental plan accomplishing the following:

- Establish the criteria and severity of a disruption based on the impact it will have on the library's critical IT functions.
- Determine what the critical IT functions and systems are and the associated timeframes for recovery.
- Determine the resources needed to support the critical IT functions and systems, and define the requirements for a recovery site.
- Identify the people, skills, resources, and supplies necessary to assist in the recovery process.
- Identify the library's vital institutional data, which must be stored offsite to support resumption of business operation.
- Document the appropriate procedures and information required for recovery.
- Provide for periodic review and updating of the plan to keep it current.
- Provide for testing of the documented procedures to ensure that they are complete and accurate.

The task force decided that a logical first step would be for each department to generate a list of its business functions. In turn, for each business function, department managers were

instructed to identify the required IT, any dependencies, criticality from both the library's and the department's perspective, and the impact on operations if IT were unavailable. The well-intended goal of creating a comprehensive inventory, however, was overwhelming and compliance was low. Within months, the project stalled and was tabled indefinitely.

Over the next year, several new campus-wide IT policies were developed and/or significantly revised, including a new enterprise backup and recovery policy and an institutional data access policy. In addition, the university's internal audit department conducted a risk assessment that spanned all university business operations, listing 13 recommendations pertaining to IT. After months of wrestling with overlapping compliance requirements, a new task force was charged with a more narrowly defined goal: to self-audit library operations for compliance with new campus recommendations and policies. The task force quickly decided that four documents should be drafted:

1. Safe Computing Policy and Practice
2. University IT Policies and Impact on Library Staff
3. Library Data Retention Schedule
4. Library IT Disaster Recovery Plan

Progress was slow but steady. The first two documents were drafted relatively quickly, but the data retention schedule and the disaster response plan took considerably longer.

Prior attempts to identify the criticality of services had always stalled because units resisted labeling any of their own functions as non-essential, leaving no guidance for the IT team on how to prioritize actions. The solution to this logjam was to avoid wasting time and energy on making fine distinctions that would be unimportant in a real-life catastrophe.

Levels of criticality were defined as: (i) critical to university operations, (ii) critical to library operations, (iii) essential, and (iv) necessary, desirable, or non-essential. By clustering "necessary, desirable, and non-essential," the task force removed the angst over labeling anything non-essential and embraced the reality that not all indispensable services are equally indispensable. Furthermore, services that fell under the cluster of "necessary, desirable, or non-essential" were not even inventoried. Volatile details such as vendor contacts, hardware and software lists, etc. were incorporated only by reference to minimize confusion from out-of-date information.

The resulting document focused first and foremost on roles and responsibilities and strategies for receiving and disseminating accurate information during a crisis. Sections included identifying who convenes the disaster response team, sending and receiving emergency communications, implementing services at a remote location, and communicating with both library staff and external constituencies. The plan was completed in February of 2008, posted for comments in March, and finalized in April. In an unlikely turn of events, it was put to the test just two months later.

Executing the Plan

Implementation of the plan can be easily divided into three distinct stages: evacuation, temporary relocation, and resuming normal operations.

Evacuation

During the week of June 9-13, 2008, the plan was invoked, the team assembled, and emergency steps taken to escape from the rising waters:

Monday, June 9, 2008. Campus officials decided to evacuate the low-lying arts campus, including the art and music libraries. Library staff and essential resources (e.g., course reserves)

were moved from those two libraries on the west bank to the presumed safety of the main library on the higher elevation east side. Since both the art and music libraries were on upper floors of their respective buildings, there was almost no risk of flood water damaging the collections, but any resources left behind could become inaccessible for an extended period. Library management began to assess the risk to the main library, but the likelihood of evacuation was very low. Engineers projected flooding at the same level as 1993, not putting the main library building at risk. Library IT staff met to discuss worst-case scenarios. For the most part, library employees responded to the campus call for volunteers to sandbag areas considered to be at risk.

Tuesday, June 10, 2008. Library special collections and archives staff decided to move any materials sitting on the floor in the basement to higher ground. Library IT staff identified in broad terms what preventative steps to take in the unlikely event library IT services needed to be relocated.

Wednesday, June 11, 2008. The evacuation of the arts campus was complete. Art and music library staff settled into their temporary quarters in the main library. No additional library resources appeared to be at risk.

Thursday, June 12, 2008. Early in the day, university officials announced that any valuable materials in 12 more buildings, including the main library, should be moved to higher ground. By mid-morning, library administrators issued the call to clear the lowest shelves in the basement, and by mid-afternoon additional shelves were added to the list. At the end of the day, campus officials indicated their intent to evacuate the main library in two days.

The library IT disaster plan was invoked and the response team was identified. The team's initial communication to library administration stated that "our expected worst-case

scenario from a library IT perspective is this: Main Library building is without utilities for an extended period of time, but the campus as a whole remains operational."

This was certainly not the worst case from a campus perspective, but was reasonably the worst case for library IT for this reason: if the overall situation on campus became truly catastrophic, problems would be so widespread that other infrastructural contingency plans would take over, giving the library IT disaster response team more time to reassess the situation. If, however, the campus remained operational and classes and research activities continued while the main library was out of commission, the technology needs would fall chiefly on library IT.

In order to prepare for this projected worst-case scenario, services in the top tier – "critical to university operations" – were copied from a virtual server environment to two physical servers. Those two servers were relocated to the College of Engineering's data center where they could be brought online if the situation deteriorated. Arrangements were made with campus network engineers for an emergency VPN that could route the library's IP subnet to the engineering building so that vendors' IP-based authentication would be preserved. Preparations were substantially completed by the end of Thursday, and a cutover could take place any time as needed.

Friday, June 13, 2008. The situation on campus deteriorated quickly after another night of severe weather. Teams of volunteers – including students and staff, townspeople, members of the local Amish community, and prisoners on release programs – descended upon the main library to sandbag the building's perimeter and formed book brigades in every stairwell to move physical collections to upper floors. The building would need to be shuttered by the end of the day with no guess when it might reopen. On the one hand, a key benefit of campus being downstream from the reservoir is that flooding is usually mitigated. On the other hand, when flooding does

occur it can persist for days or weeks. Back in 1993, water poured over the spillway uncontrollably for four weeks.

With top-tier services in good shape, the library IT disaster response team quickly developed plans to restore the second tier – "critical to library operations" – which included access to networked drives, intranet, and desktop computers. In the event that the library would need to operate for weeks or months at a remote location, plans were made to relocate the entire data center, moving two complete racks out of the building to higher ground. The library's server room was itself not in danger of flooding barring an unimaginable catastrophe. If the water reached the building, however, power and networking would be unavailable.

The team decided that the best option for fully operating at a temporary location would be simply to relocate existing production equipment. With several hours remaining before building closure, there was time to power the servers down gracefully and move equipment to the College of Engineering. The racks could not be transported while fully populated due to the weight of hard drives and backup power supplies. Under close supervision of the library's lead system administrator, a team of volunteers – mostly programmers from central IT – helped tear down the servers and carefully transport drives, battery supplies, and half-empty racks to the engineering building. At the same time, another team of volunteers – mostly academic technology staff from central IT – helped move 150 desktop computers and monitors to a storage area. As luck would have it, a new fleet of library computers had just arrived and were still in their original boxes, making it easy to transport several dozen computers. Fortunately, librarians for the most part had adopted best practice and kept essential work-related files on network storage, so individual desktop hard drives were not a priority.

To the outside world, library servers appeared offline for just a few hours – from the time network engineers removed building switches when underground utility tunnels were breached until the VPN that routed the library's subnet to the engineering building was activated. Top-tier services "critical to university operations" were fully online by the end of Friday, and second-tier services "critical to library operations" were available by end of Saturday.

Temporary Relocation

During the following week, June 16-20, campus was closed to all but essential personnel. The official campus list of "essential personnel" was born out of pandemic flu planning and appropriately focused on personal safety and medical communications. The university adjusted quickly recognizing that "essential personnel" varies depending on the situation at hand. Library IT staff worked throughout the week to get temporary systems in place so that nearly all library operations could resume when campus reopened. By Friday, June 20, several more servers were back online. Temporary offices were set up: administration, finance, and human resources in the business library; circulation and reserve in the engineering library; interlibrary loan and technical services in the health sciences library; and media services in the physics library. A farm of desktops were set up to allow digital library and IT staff to telecommute over Remote Desktop Protocol; public services staff from the art, music, and main libraries worked either from home or at a bank of business library workstations repurposed for shared staff use.

Classes resumed on Monday, June 23, but the main library and two dozen other buildings remained closed. The main library was certified for occupancy on Monday, July 7, and reopened to the public on Wednesday, July 9. Overall, the evacuation went smoothly, and the library continued to serve campus from a variety of remote locations for a month. The only equipment

failure was a USB dongle that had accidentally been left attached to the server and was damaged as the server and rack were carted through a doorway.

Resuming Normal Operations

The recovery process was slow-going. Though the main library reopened to the public in a matter of weeks, repairs continued for months. The art library remained in its temporary location nearly four years, finally returning home in 2012. The music library continues to be housed in temporary quarters until a new music building is finished, anticipated for the fall of 2016, fully eight years after the flood.

A story like this would typically end with returning everything to its proper home and resuming normal operations. Just as flood recovery began in earnest, however, the global financial crisis hit, further disrupting campus activities, putting flood recovery funds at risk, and prompting many discussions of "the new normal." In a *Wall Street Journal* article on November 21, 2008, then-incoming White House Chief of Staff Rahm Emmanuel said, "You never want a serious crisis to go to waste." Inspired by this sentiment, library IT staff looked for opportunities to challenge deeply held beliefs and think strategically. Staff occasionally joked about looking for ways to "turn floodwater into lemonade."

Mitigating Risk

With the promise of cloud computing on the horizon coupled with some unexpected personnel changes, the campus challenge to seek new ways of doing business became a catalyst for reimagining the library IT server infrastructure and moving library IT services to hosted platforms.

Though significant resources had been spent over the past few years constructing a new server room and upgrading equipment, the flood was a visual reminder that, from the campus

perspective, a small departmental server room is not an institutional priority. The sandbag wall keeping the river from the library was impressive. But the sandbag wall on the other side of the library – the one protecting the campus data center – was built to a much higher elevation. During the flood, the library's servers were relocated to the College of Engineering's data center, a superb environment with a fully redundant electrical system, yet even there they needed to be shut down briefly when the chilled water system failed. The message was clear: to maximize the chance of staying online, or coming back online after a catastrophe, library systems could not remain isolated.

Several library IT services, such as interlibrary loan, have been migrated to vendor-hosted platforms – albeit with the usual mixed reviews. Library systems remaining on premise have now been permanently relocated to server farms in more centrally managed data centers.

One of the most significant post-flood infrastructural improvements was a new state-of-the-art enterprise-wide data center that came online in 2012. Due to some service-level limitations, some library systems remain under the care of the College of Engineering, but the rest have been moved to the new data center. In 2013, the library's server room was powered down once and for all.

These cloud-based solutions created new dependencies and triggered significant revisions to the library IT disaster response plan. The library no longer owns any server hardware, although relinquishing local control has its own disadvantages and requires new and different strategies for disaster response.

Lessons Learned in 2008

Lesson #1: Plans may be worthless, but planning is indispensable.

The disaster response plan was helpful in defining priorities and setting expectations. The lack of specificity in the plan was not only not problematic but kept the document relevant in an unanticipated situation. Former U.S. President Dwight D. Eisenhower once stated: "I tell this story to illustrate the truth of the statement I heard long ago in the Army: Plans are worthless, but planning is everything. There is a very great distinction because when you are planning for an emergency you must start with this one thing: the very definition of 'emergency' is that it is unexpected, therefore it is not going to happen the way you are planning. So, the first thing you do is to take all the plans off the top shelf and throw them out the window and start once more. But if you haven't been planning you can't start to work intelligently at least. That is the reason it is so important to plan, to keep yourselves steeped in the character of the problem that you may one day be called upon to solve – or to help to solve."[3]

By not trying to identify every service and not worrying about subtle distinctions between necessary or desirable, the written plan stayed focused on broad concepts, trusting that the implementation team would work out the specifics based on the situation at hand. Too much detail makes a plan less applicable in unanticipated circumstances.

Lesson #2: In any given disaster, probabilities don't matter.

A Galton board, sometimes referred to as a "bean machine," nicely illustrates the central limit theorem where any large number of trials will trend toward a normal distribution curve.[4] But the tool also illustrates that it is not possible to predict the outcome for any single trial. There is a temptation to spend time planning the "most likely" scenarios. A given disaster, however, is just one random experiment. As the disaster unfolds (or as the ball drops down the Galton

board), it is easy to account for all possible next moves. There is, however, neither time to plan for every outcome nor benefit in guessing outcomes based on a false premise of the "typical" situation. No disaster is typical.

Lesson #3: Name a non-essential team member for communications.

The disaster response plan appropriately described how official communications will be delivered and received, naming the authorities for official information. During a crisis situation, however, there is an additional need to identify personnel who can serve in a dispatch role. These individuals do not need subject expertise or authority. In fact, IT skills are a disadvantage because of the temptation to pull these individuals away from dispatch. This gap of a non-essential team member was especially noticeable when trying to coordinate with external units who were also busy dealing with the disaster. The library needed a place to stow 150 desktop computers and monitors and a potential location was identified. However, key personnel at that location could not be reached and there was no reliable way to "leave a message." A non-IT person who could be dispatched to establish contact and close the deal would have been invaluable.

Lesson #4: Identify a volunteer coordinator.

When drafting the disaster response plan, no one had considered how to handle volunteer offers for help, yet during the evacuation volunteers kept pouring in. Some had no special IT skills and could get redirected to other efforts such as sandbagging or book brigade, but dealing with these individuals took time away from attending to IT needs. A few volunteers were IT professionals who wanted their IT skills to be put to good use and were tapped to help with moving servers.[5] Coordinating the many unexpected volunteers was, at times, overwhelming.

Lesson #5: Essential is a relative concept.

The notion of identifying "essential personnel" was first introduced in pandemic flu planning and carried over to other critical incidents. Upper-level administrators and health and safety experts were deemed essential, but IT support staff were not. This confusion was an early barrier that was quickly eliminated. Even among IT staff, the notion of who was essential would vary as the crisis unfolded. At times, desktop support staff or web editors suddenly became essential.

Similarly, despite best effort to list all essential services, circumstances on the ground can quickly change what is deemed essential. While drafting the disaster response plan, interlibrary loan was seen as very important but was not a top priority. With no access to the physical collections, however, the relative importance of interlibrary loan suddenly increased.

Lesson #6: Prepare for personnel changes among the disaster response team.

Core team members were selected based on skills and availability, but the catastrophe introduced new unexpected variables. No one had imagined, for example, that it would become important to consider which team members lived on which side of the river, a factor that came into play once the last remaining bridge in Iowa City was threatened to close. Several library staff members commute to Cedar Rapids, normally a 25-mile drive. But with road closures the detour became a 250-mile trip.

Lesson #7: Look for easy opportunities to repurpose resources.

Outside of the library, staff in other campus buildings were instructed to pack up their desktop computers. The library, however, had just received new computers yet to be deployed. This allowed non-IT staff to participate in other disaster response activities (such as relocating special collections materials) rather than unplugging and boxing their desktops. In a debriefing

after the event, staff noted that another solution would have been to repurpose student checkout laptops and issue them to library staff on their way out the door. The disaster response plan should explicitly grant authority to one or more members of the team to make last-minute administrative decisions that might contradict standing policy.

Observations from 2013

The Iowa River rises every spring, but in 2013 the water level once again triggered the flood response plan. No IT actions were required, but the weather outlook was grim and it was not unreasonable to ponder another building evacuation.

The prospect of relocating library staff and library IT operations a second time seemed overwhelming. But how could that be? With all the lessons learned from 2008, an updated disaster response plan, and time and effort moving to a centralized data center, it would seem that riding out a repeat catastrophe should be straightforward, but it would not have been.

Observation #1: Preparedness and readiness are different.

FEMA provides families with a wealth of information about planning and preparing for disasters and emergencies (www.ready.gov). Families with a communications plan, an emergency kit, and a well-constructed home may be equally prepared for a tornado or a hurricane, but the steps for weathering each storm are quite different. Those in the path of a hurricane typically have a few days to get ready, whereas a tornado forms quickly and causes damage only while it touches ground. Hurricane warnings are issued 36 hours in advance; tornado warnings sometimes come after the fact.

With the benefit of hindsight, the library's preparedness was equally strong in 2008 and 2013. The digital library was never at risk. Had there been a sudden flood in 2008, the damage would have been unimaginable but still completely reversible. The reservoir upstream, however,

made Iowa City's flood experience more like a hurricane. A 36-hour warning still leaves 36 hours of work to do. Better preparedness might mean top priorities are in good shape, but there are always plenty of second, third, and lower priorities calling for reinforcement.

Observation #2: Planned obsolescence changes the calculus.

A disaster response plan for library IT may look immature when held up against a plan for physical collections. The foundation upon which each is built, however, is characteristically different. The envelope that encloses the physical collection (the library building) is constructed on a promise that it will serve its purpose well for 50 or 100 years. By contrast, the envelope for the digital collection (the library IT infrastructure) is unashamedly built on the premise of planned obsolescence.

One might imagine how overwhelming the task of writing a disaster response plan for the physical collection would be if odds were high that another two or three buildings will be constructed with two or three moves from one to the next in between any two disasters. While planned obsolescence is not an excuse for avoiding the hard work of creating and regularly a plan, it does change what is important. Detailing vendor contact lists and documenting dependencies of dependencies is not time well spent. The IT experts in charge of recovery will never trust a list that was outdated as soon as it was printed. Plans for emergency communications, however, are paramount since even in the best of times, communications between IT and non-IT can be challenging. Inability to access the physical collection is self-evident when water is surrounding the building or the National Guard is directing traffic, but information regarding IT unavailability can be hard to come by when the technology that enables communication is unavailable.

Observation #3: No digital asset is original.

With physical artifacts, deciding what to rescue first can be complicated because the value of an artifact varies based on who is doing the valuation. The concept of an item having a fair-market value is predicated on an assumption that an acceptable alternative can be proffered. A replacement might be indistinguishable from an original, but in a literal sense it is materially different.

Libraries tend to rely on these familiar labels when they talk of "unique digital collections" and safeguarding "preservation masters," losing sight of the subtlety that digital files are literally immaterial; the first time a file is saved to disk it is already a copy. In day-to-day operations, this distinction is meaningless. The strategy for mitigating against loss of information on disk is multiple copies and frequent backups. No one experiences grief for the loss of a file when another copy is successfully recovered from tape.

While bracing for an impending disaster, however, the lack of originality in a digital file is more salient. In 2008, hundreds of volunteers descended upon the library to save the collection. For months afterward they told story after story about book brigades and how big the library is and the arcane dissertation titles they passed from hand to hand. Yet no one was moved to ask about the digital library. On the one hand, hundreds of people were needed to save the print collection; on the other hand, hundreds eagerly volunteered.

The overarching takeaway from both the 2008 flood and the 2013 near-miss is the extent to which a library IT disaster response plan is not particularly valuable as a technical resource. Certainly a plan needs sufficient detail to enable an IT professional unfamiliar with the environment to step in. But IT professionals solve IT problems for a living, so trying to solve

imaginary problems ahead of time is not a priority. Rather, the most indispensable sections of the plan are the default solutions to non-technical issues – organizational structure, lines of authority, and most importantly human relations.

---

[1] The University of Iowa, President's Forum: Flood Report – 2008. http://www.uiowa.edu/floodrecovery/recovery-reports/president-forum-090908.pdf.
[2] Board of Regents State of Iowa, University of Iowa Flood Recovery – Updated Cost Estimates, 2009. http://www.regents.iowa.gov/Meetings/DocketMemos/09Memos/March/0309_ITEM14d.pdf.
[3] United States, and Dwight D. Eisenhower, *Public papers of the Presidents of the United States: Dwight D. Eisenhower; containing the public messages, speeches and statements of the President, 1953-[1960/61]* (Washington: U.S. Govt. Print. Off., 1958): 818.
[4] Barile, Margherita and Weisstein, Eric W. "Galton Board." From *MathWorld* – A Wolfram Web Resource. http://mathworld.wolfram.com/GaltonBoard.html.
[5] There was a humorous miscommunication when a call for volunteers to handle fragile hard drives was relayed as a request to deal with sensitive data.