

Disaster-Proofing the Library

From incident lessons to a usable preparedness plan

Companion case study for *Disaster-Proofing the Library: Leadership, Policy, and Technology Resilience*

Robin Hastings • September 28, 2026

Kansas Library Association Conference • October 29, 2026

Technology disasters are no longer solely “IT problems.” When systems become unavailable, library leaders still have to decide what services can continue, who has authority to act, and what staff and patrons need to know. A plan becomes useful when people can find it, follow it, and demonstrate that it works.

This companion draws on the presentation's three historical library cases and turns their lessons into a starting sequence for directors, managers, supervisors, and boards. The implementation steps are proposed practices for a library to adapt. They are not a report of work completed at NEKLS or evidence of results produced by the presentation.

The challenge

A library can have a backup subscription, a technology vendor, and a disaster plan and still be unable to answer basic recovery questions. Who can authorize an emergency expense when the director is unavailable? Which services can operate without the catalog? Can someone other than the usual technical contact locate the instructions? What would count as successful restoration?

The presentation approaches these questions through governance, continuity planning, access and privacy policies, vendor expectations, communication, and staff practice. Its contribution is to connect technical dependencies to decisions library leaders can make and verify.

Three cases and their documented outcomes

Toronto: keeping some services available

Toronto Public Library's November 14, 2023 update said the incident first came to its attention on October 28. Branches remained open, and materials could be borrowed, returned, or renewed. Public computers, printing, online personal accounts, and holds management were unavailable. The update also described stolen staff-related information and an investigation that was still underway.

Documented outcome: Some public services continued while other services and access to systems remained disrupted. This was partial continuity, not full recovery.

Application for a smaller library: Define availability service by service. Decide what staff can offer safely, what must pause, and how patrons will learn the difference. [Toronto Public Library, November 14 update](#)

British Library: backup data still needs a working environment

The British Library's March 8, 2024 review described the aftermath of its October 2023 attack. It reported viable backup sources for collections and other data, but a shortage of viable infrastructure on which to restore them. Legacy applications, technical obsolescence, and vendor support limitations complicated recovery.

Documented outcome: Buildings remained open and a searchable main catalog became available on January 15, 2024, but services were still incomplete when the review was published. Backup availability did not mean the whole service was recoverable immediately.

Application for a smaller library: Ask for a demonstration of a usable service, including its software and dependencies. A successful file copy does not answer whether staff can do their work. [British Library cyber incident review, pp. 7-9](#)

Seattle: making recovery visible

Seattle Public Library's public update page tracked services affected by the ransomware attack that began over Memorial Day weekend in 2024. Its September 4 update reported restoration of affected public services and listed availability across account, collection, technology, and other services. It also identified an interim solution for online library card registration.

Documented outcome: The library reported restoration of affected public services by September 4, with service-specific qualifications. That statement does not establish that every internal system or investigative activity was complete.

Application for a smaller library: Maintain a dated service-status list that distinguishes available services, temporary arrangements, and remaining limitations. [Seattle Public Library, update last revised September 4, 2024](#)

These cases illustrate different recovery problems. The applications above were synthesized and summarized for this companion.

Implementation: start with one essential service

The sequence below expands the presentation's planning and practice sections. Suggested owners are roles to assign locally, not new commitments for any named person. Small libraries may combine roles, but should still name an alternate.

1. Decide what must continue

Suggested owner: Director with public-service and administrative staff.

Choose one essential service and describe the minimum useful version of it during an outage. Include the people, systems, data, facilities, and vendors it depends on. Agree on how long disruption can be tolerated and what temporary arrangement is acceptable. Include administrative needs such as payroll when deciding priorities.

Output and check: A one-page service record. A colleague should be able to explain what continues, what pauses, and what would trigger a new decision.

2. Put authority and contacts in writing

Suggested owner: Director, with board involvement where local authority requires it.

Name the incident lead and alternate. Record who may approve emergency spending, pause or resume a service, contact technical support, and approve public statements. Confirm vendor escalation contacts. Keep essential instructions securely accessible when the ordinary network or email is unavailable.

Output and check: A decision-and-contact sheet. Ask the alternate to locate it and explain the first decisions without help from the usual lead.

3. Review access and temporary privacy practices

Suggested owner: Designated access administrator with the director and service supervisor.

Review who has access to the selected service, including vendors. **Identify obsolete permissions, shared accounts, and responsibilities for staff departures.** Agree on how any manual workflow will limit collection of patron information, protect the records, and reconcile them when systems return. Resolve retention questions under the library's existing policy.

Output and check: An access review and a short fallback procedure. Walk through a sample transaction with fictitious information and identify who can see each record.

4. Establish what recovery actually requires

Suggested owner: Technical provider or IT staff, with a library service owner.

Ask who backs up the data, who restores it, and what software, licenses, equipment, and accounts restoration requires. Agree on a controlled test outside production. Have library staff validate a representative transaction, not just the presence of recovered files. Record elapsed time, the age of recovered data, failures, and dependencies requiring follow-up.

CISA's October 2023 guide recommends offline, encrypted backups and regular tests of their availability and integrity. It also recommends maintaining and exercising incident-response and communication plans, including offline and paper copies. [#StopRansomware Guide, pp. 5-6](#)

Output and check: A dated recovery-test record. Compare the observed result with the library's service requirements; record unresolved gaps rather than calling the service fully recoverable.

5. Prepare the first service update

Suggested owner: Designated spokesperson and alternate.

Prepare a message structure covering what is known, what patrons can use, what remains unavailable, and when the next update will appear. Identify a communication channel that remains accessible if the usual website or email fails. Ensure frontline staff receive the same confirmed information.

Output and check: A draft update and a service-status list. Have a colleague check whether the message answers a patron's immediate questions without promising an unsupported recovery time.

6. Practice, repair, and repeat

Suggested owner: Incident lead with staff who deliver the selected service.

Use the presentation's scenario: the catalog and staff email are unavailable before opening, and the director cannot be reached. Discuss who leads, what remains available, how staff communicate, and how patrons receive updates. Keep this a discussion exercise; **do not disable live systems during this test.**

Record the points where people lack information or authority. Choose a manageable improvement, assign an owner and locally agreed completion date, and repeat the relevant part of the exercise after the change. Encourage staff to identify confusing procedures and mistakes without fear of public blame.

Output and check: An exercise record with gaps, decisions, and follow-up results. Completion means the revised procedure has been demonstrated, not merely rewritten.

A service record participants can reuse

Field	What to record
Essential service	The specific service and who depends on it
Minimum service during disruption	What remains available and what pauses
Lead and alternate	Roles, current contacts, and decision authority
Dependencies	Systems, vendors, accounts, software, people, and facilities
Temporary procedure	Staff instructions and privacy protections
Recovery requirement	Tolerable interruption and acceptable age of recovered data
Evidence	Test date, conditions, observed result, and who verified it
Remaining gap	Required improvement, owner, and locally agreed review date

Begin with one completed record and one practice session. Expand to other services as staff learn what the process requires. Low-cost work still needs staff time, and some gaps will require technical support or funding.

Outcomes: what can be supported

A library using the companion can build evidence in stages:

Intended improvement	Evidence to collect	What that evidence can establish
Staff can find the plan during an outage	An alternate retrieves the current copy without normal network access	Accessibility under the tested conditions
Decision authority is understood	Exercise notes show who made each required decision and where escalation stalled	Which responsibilities are clear and which need revision
An essential service can be recovered	A controlled test restores data and a representative transaction works	Recovery capability for the tested service and conditions
Patrons receive usable information	A reviewed update identifies available services, limitations, and the next update	Message completeness; not proof of increased public trust
Follow-up changes work	A repeated exercise demonstrates that a recorded gap has been resolved	Verified improvement in that procedure

Record a baseline before making an improvement if a later comparison is needed. A faster repeat exercise should be described as an exercise result, not as a demonstrated reduction in real incident downtime.

Audience takeaways

- Leadership defines service priorities, authority, and acceptable temporary operations.
- Vendor assurances become useful when responsibilities and recovery evidence are specific.
- A plan must remain accessible when ordinary systems fail.
- Practice should reveal gaps, with time and ownership assigned to address them.
- Start with one service and one demonstrated improvement.

Source and editorial notes

Historical claims above use dated primary-source accounts; they are not statements of current service status. Sources were checked September 28, 2026.

- **Presentation basis:** Robin Hastings, *Disaster-Proofing the Library: Leadership, Policy, and Technology Resilience*, prepared for the Kansas Library Association Conference, October 29, 2026; 33 slides and speaker notes, with the presentation outline. [Presentation information and resources](#). The implementation sequence expands slides 10-31; the practice scenario comes from slide 27.
- **Toronto source limitation:** The linked page is an official-domain retained copy under a test path, titled “Toronto Public Library Website Update bk.”
- **British Library source boundary:** The March 2024 review describes recovery in progress. Its projected restoration dates are not treated here as completed outcomes.
- **Seattle date distinction:** The page was first published May 28, 2024, and updated September 4. The restoration statement belongs to the September update.
- **CISA access:** The cited October 2023 primary-source guide was read from the U.S. Treasury CDFI Fund's hosted copy because CISA's direct page and PDF did not load. It supplies background guidance, not proof of outcomes at the three libraries.
- **Review status:** Prepared from Robin's work on the upcoming Tech Disaster book with assistance from her AI Agent. The final review and publication were approved and owned by Robin. No participant evaluation or local implementation result is represented as completed.