Anatomy of a Crisis:

Deconstructing the British Library Cyber Attack

Databarracks

Contents

Executive summary

In October 2023, the British Library was hit by a ransomware attack that took down most of its online systems and caused long-lasting disruption across the Library's services. It is widely regarded as one of the most damaging cyber incidents to affect a UK public institution and a notable case globally in the cultural heritage sector.

The Library's forensic investigation concluded that the most likely entry point was a remote access server without multi-factor authentication – a known risk that had been identified but not fully addressed. The attackers exfiltrated around 600GB of data, including staff and user information, and encrypted and destroyed much of the Library's server estate. Recovery has cost at least £7 million – more than 40% of the Library's unallocated reserves.

The attack was claimed by the Rhysida group, which operates a double extortion model, combining data theft with system encryption. When the Library refused to pay a 20 bitcoin ransom – worth around £600,000 at the time – the data was first put up for auction and later published on the dark web.

The disruption cut across the Library's core services, forcing staff to revert to pen and paper processes while access to collections – particularly digital and research services – was heavily restricted. The loss of systems was debilitating for the Library, which holds more than 170 million items, including every print and digital work published in the UK. Senior leadership described the impact as comparable to the loss of the Library of Alexandria, reflecting the scale of operational and cultural disruption. The experience was also described as traumatic for staff, with lasting effects on wellbeing as well as operations.

Recovery was prolonged by the condition of the underlying technology. As a 50-year-old institution with a complex and evolving IT estate, the Library relied on a large number of legacy systems, many of which could not be restored in their original form. This meant systems had to be rebuilt or replaced rather than restored, turning recovery into a multi-year programme and driving costs to more than 10 times the original ransom demand.

The British Library published an unusually detailed post-incident review in March 2024, providing one of the clearest public accounts of a major ransomware attack. The Information Commissioner's Office (ICO) and National Cyber Security Centre (NCSC) both commended this transparency, highlighting the value of sharing detailed lessons to support wider resilience. The NCSC also praised the decision not to pay the ransom, reinforcing UK policy discouraging payment.

The publication of the report did not mark the end of the recovery, however. More than two years on, the Library is still restoring systems and services. A structured Rebuild & Renew programme was established to replace infrastructure, restore services and modernise the technology estate.

While the attack was unusually destructive, the underlying issues were not unique. The incident reflects wider challenges across public sector and cultural institutions – including reliance on legacy systems, stretched technology teams and constrained cyber security investment.

The British Library's own review highlights clear lessons: implement multi-factor authentication across all access points, segment networks to limit impact, rehearse for total system loss and prioritise recovery capability alongside prevention.

Drawing on publicly available sources, this report examines how the attack unfolded, the impact across the business and the road to recovery. It also sets out the key resilience lessons for organisations facing similar risks.

Timeline of events

This timeline reconstructs the key events of the British Library cyber attack from publicly available evidence, tracing the incident from initial access through to recovery.

Date	Event	Impact
25 October 2023 (or sooner)	Initial access and reconnaissance activity on the network, with attackers likely present at least 3 days before detection.	Attackers establish a presence and operate undetected prior to discovery.
28 October 2023 (early hours)	Large volumes of data leave the network, later linked to the exfiltration of around 600GB of files.	Data theft completed prior to detection, enabling double extortion.
28 October 2023 (morning)	7:35am: Intrusion identified as major incident. 9:15am: The Library's Business Continuity Manager invokes the crisis management plan. 10am: Gold command convenes via WhatsApp, with email unavailable. NCSC and Department for Culture, Media and Sport (DCMS) are informed.	Major incident formally identified and escalated to executive crisis response under degraded communications.
28 October 2023	2pm: NCSC attends a subsequent Gold meeting and provides early advice on incident handling, including communications strategy. Specialist cyber security firm, NCC Group, is engaged following consultation with NCSC. Servers and online systems are taken offline. Forensic investigation begins. Physical security and fire safety systems remain operational and public spaces stay open.	Containment action limits further spread but causes immediate loss of digital services.

Timeline of events

28–30 October 2023	Manual workarounds are introduced, including paper-based processes in Reading Rooms. Access to collections is heavily restricted and deliveries from Boston Spa, which houses more than 75% of the collection, are paused.	Core services are severely degraded and access to a large share of physical holdings is disrupted.
29 October 2023	The Library posts on X that it is experiencing "technical issues" affecting its website, phone lines and onsite services. Technology teams begin resetting accounts and collating breach information for the ICO.	First public sign of the incident; service disruption becomes visible and regulatory response begins.
30 October 2023	Onsite backups confirmed compromised and encrypted. The loss of control of data is reported to the ICO. Copies of key digital content, including data held within the Digital Library System (DLS) and UK Web Archive, are confirmed safe.	Loss of viable backups removes rapid recovery options, but core collection data remains recoverable.
31 October 2023	The Library publicly confirms it has suffered a cyber attack and continues working with NCSC and law enforcement.	Incident formally acknowledged and escalated to a national-level response.
20 November 2023	Rhysida claims responsibility and launches a dark web auction for stolen data.	Attribution confirmed; extortion phase becomes public.
27 November 2023	After the Library refuses to pay the ransom, the stolen data is published on the dark web.	Data exposure risk materialises for staff and users, with long-term consequences.
December 2023	Viable backup sources for collections and metadata are identified. The Library begins transitioning from Gold/Silver crisis management to structured recovery.	Recovery becomes possible, but only through a staged rebuild rather than rapid restoration.
20 December 2023	Board approves Rebuild & Renew programme.	Establishes structured, long-term recovery and rebuild strategy.
15 January 2024	Main catalogue restored in limited read-only format.	Partial service restoration; core functionality still constrained.

Timeline of events

8 March 2024	The British Library publishes its Cyber Incident Review.	Provides one of the clearest public accounts of a major ransomware attack and sets out lessons for the sector.
16 August 2024	The Library publishes a £400,000 tender for the first phase of its Web Foundations project, seeking a partner to replace the interim website with a more robust, scalable and secure platform.	Marks transition to funded infrastructure rebuild.
2024–2025	Ongoing phased rebuild of systems, infrastructure and services.	Recovery extends over multiple years due to rebuild requirement.
30 April 2025	The ICO concludes its consideration of the case, commends the Library's transparency and states that further investigation would not be the most effective use of its resources.	Regulatory scrutiny closes without further action, while reinforcing the value of openness and lessons shared
21 November 2025	A public restoration update confirms that recovery is ongoing, with further key services due to return in late 2025 and early 2026.	Confirms long-tail recovery and sustained operational impact
Late 2025	*The Independent* reports that ongoing disruption from the cyber attack is a contributing factor in staff industrial action, with continued impact on workload.	Ongoing fallout from the attack continues to affect staff workload and morale.
15 December 2025	New main catalogue platform launched, alongside an interim Archives and Manuscripts Catalogue.	Marks transition from workaround solutions to rebuilt core infrastructure.
January 2026	Interim Chief Executive Jeremy Silver says the Library is "starting to turn a corner", with most remaining services expected to return during 2026.	Recovery is nearing completion, but remains ongoing more than 2 years after the attack
9 April 2026	Electronic legal deposit material catalogued before October 2023 becomes available again in Reading Rooms.	Restoration of a part of the Library's research offer

Adversary

The attack on the British Library was claimed by Rhysida, a ransomware-as-a-service operation that emerged in 2023 and is thought to have links to Russia and former Soviet states.

CISA notes that Rhysida focusses its attacks on “targets of opportunity” across sectors including government, education, healthcare, manufacturing and IT. In practice, that means targeting organisations where attackers can gain maximum leverage against minimum resistance – especially those that hold sensitive data and depend on continued access to systems.

Reported victims include the Chilean Army, the City of Columbus, Ohio, Insomniac Games, MarineMax, King Edward VII’s Hospital in London and Energy China.

Modus operandi

Like other ransomware groups, Rhysida uses double extortion tactics to pressure victims into paying a ransom demand in bitcoin. This combines system encryption with the theft of sensitive data and the threat of its publication. In ransom notes, the group has presented itself as a “cybersecurity team”, claiming to help victims identify weaknesses in their systems while demanding payment.

The British Library’s review describes Rhysida’s attack methodology as combining defence evasion and anti-forensics, exfiltration of data for ransom, encryption for impact and destruction of servers to inhibit recovery. The attackers “clean up after themselves” by deleting logs and obscuring their presence, making investigation and attribution harder.

Rhysida attacks typically involve:

- Initial access through compromised credentials or external-facing services
- Lateral movement using legitimate administrative tools
- Targeted identification and extraction of sensitive data
- Deployment of ransomware to encrypt systems
- Destruction of infrastructure to inhibit recovery
- Extortion through ransom demands and threats of data publication

At the British Library

In this case, attackers exfiltrated approximately 600GB of data – equivalent to just under half a million documents – before encrypting systems and destroying large parts of the Library’s server estate. They carried out targeted searches across the network, scanning for files using sensitive keywords such as “passport” and “confidential”, and copying data from both corporate systems and personal storage locations.

The group advertised the stolen data as “exclusive, unique and impressive” and published sample images of employee documents, including passports, on its leak site to increase pressure on the Library to meet its ransom demand.

Impact

Ciaran Martin, former CEO of the NCSC, has described the attack on the British Library as "one of the worst cyber incidents in British history".

The impact was felt immediately and described by the Library as "deep and extensive across all areas of Library activity, with users, staff and key stakeholders almost all affected."

Since 2015, the Library has measured performance against six core purposes: Custodianship, Research, Business, Culture, Learning and International. The most severely affected by the attack were Custodianship and Research, which were both graded "red/amber".

Operational

When the Library reopened on the Monday after the attack, it had effectively returned to a pre-digital state. The online catalogue, website, internal systems, phone lines and public wifi were all unavailable. Manual workarounds were introduced immediately to sustain operations.

Access to collections was significantly reduced in the weeks that followed. Deliveries from Boston Spa – which houses more than 75% of the Library's holdings – were paused, limiting access to a large proportion of physical materials.

Digital access was more severely affected, with research services including e-resources, online journals and EThOS (E-Theses Online Service) unavailable in the immediate aftermath of the attack and significantly restricted even after the return of a searchable version of the catalogue on 15 January 2024.

Some core functions continued despite the disruption. Security systems were unaffected, allowing buildings to remain open to the public throughout the incident. Exhibitions and public events went ahead as planned and in some cases exceeded targets. Cloud-based systems, including finance, HR and payroll, also continued to function throughout.

Financial

The attack had a significant financial impact, with recovery costs reaching at least £7 million – more than 10 times the £600,000 ransom demand and equivalent to more than 40% of the Library's £16.4 million unallocated reserves.

The Library was commended for its decision not to pay any ransom. While doing so would not have guaranteed restoration or prevented data release, the decision meant the Library knew it would have to absorb the full cost of recovery.

The need to rebuild rather than simply restore systems brought forward planned investment in infrastructure modernisation and legacy system replacement. Additional costs arose from external cyber security support, while disruption to online ticketing reduced income.

This took place against a backdrop of long-term funding pressure, with real-terms funding having fallen by around 40% over the previous 20 years.

Legal and regulatory

The attack resulted in the theft and publication of personal data belonging to staff and users, which triggered reporting obligations under UK data protection law.

The Library reported the breach to the Information Commissioner's Office (ICO) in late October 2023 and engaged with regulators and law enforcement throughout the incident.

In April 2025, the ICO concluded its consideration of the case, commending the Library's transparency and determining that further investigation would not be the most effective use of its resources.

Reputational

The Library's decision to publish a frank and detailed account of the attack, including an admission of shortcomings in protection and response, helped to limit reputational damage.

Both the NCSC and ICO highlighted the value of the report in helping other organisations understand and prepare for similar attacks. Such transparency is unusual in the wake of cyber attacks and has positioned the Library as a leading case study.

At the same time, the attack prompted criticism that, given the importance of its collections, the Library had not been adequately protected, drawing attention to broader concerns around cyber resilience across the galleries, libraries, archives and museums (GLAM) sector and public institutions.

While the Library's transparency helped protect its overall reputation, confidence among its most affected stakeholders has been more difficult to sustain. As recovery has extended from months into years, staff and researchers, many of whom were initially sympathetic, have become increasingly frustrated and, in some cases, vocally critical.

The human cost

The attack had a direct and lasting impact on staff at the British Library. Sensitive personal data was stolen, including passport scans, and published online by the attackers.

This was an ongoing source of anxiety in the months that followed, with affected staff receiving fraudulent messages as well as marketing and scam calls. Some felt compelled to take protective measures, including changing passports or addresses.

At the same time, staff had to keep services running under degraded conditions while managing user frustration. Many were unable to perform important parts of their roles or were required to follow what the Library described as "more onerous manual processes", with core tasks carried out using paper-based workarounds.

More than two years on, staff continue to deal with the effects of the attack, including increased workload and ongoing system limitations.

Response

The Library moved quickly to contain the attack, escalating to crisis management structures, taking core systems offline and starting forensic investigation with external cyber security support.

An early decision was taken not to pay the 20 bitcoin ransom, aligning with UK government policy and NCSC guidance and setting the direction for crisis management and subsequent recovery efforts.

Initial response and containment

The attack was identified on the morning of Saturday 28 October 2023. Within hours, it was escalated as a major incident, and the Library's crisis management plan was invoked.

Gold and Silver command structures were convened to coordinate the response.

The NCSC was informed immediately, and specialist cyber security firm NCC Group was engaged to support containment and forensic investigation.

Core systems, including servers and online services, were taken offline to contain the attack. This prevented further spread but resulted in immediate and widespread disruption. It also meant that manual workarounds had to be introduced to maintain services.

Crisis management under disruption

The Gold/Silver command structure replaced normal management arrangements and remained in place until the situation stabilised in mid-January 2024.

A year after the attack, the NCSC commended the Library's response, noting that the impact could have "been much worse" and highlighting the Library's "well-prepared incident response plan" which enabled "a swift, effective response".

Crisis communications and transparency

Communications were managed under heavy constraints, with the website and intranet initially unavailable. Early updates were issued through social media and internal messaging, before expanding to email communications, FAQs and an interim website as systems stabilised.

Following NCSC guidance, communications balanced transparency with the need to avoid disclosing information that could assist the attackers. External updates focussed on service availability, setting out clearly what was operational, restricted or unavailable.

Staff were prioritised in communications, receiving updates ahead of public announcements to prepare for user queries.

A high level of openness was maintained throughout the incident and its aftermath. This culminated in the publication of a detailed Cyber Incident Review in March 2024 – an approach that remains unusual in ransomware incidents and has been recognised as valuable across the sector.

Recovery

The British Library's recovery was shaped by the nature of the attack and the legacy infrastructure it destroyed. Recovery required rebuilding the Library's systems rather than restoring them. While initially structured as an 18–22-month programme, recovery extended beyond this timeframe, with some services still being restored more than two years later.

Rebuild & Renew

In December 2023, the Library moved from crisis response to recovery with the launch of the Rebuild & Renew programme, replacing the Gold and Silver command structure.

The programme set out a three-phase approach to recovery, allowing the Library to restore services through interim solutions while rebuilding core systems in parallel:

- Respond – immediate crisis management (October 2023 – January 2024)
- Adapt – interim solutions to restore services and processes (November 2023 – June 2024)
- Renew – full rebuild of systems and infrastructure (December 2023 – July 2025)

The Library framed the recovery as an opportunity to "build back with greater resilience" and incorporate lessons learned from the attack.

The programme also targeted a shift to a more modern and secure architecture, including network segmentation, stronger access controls, wider use of multi-factor authentication and more resilient backup arrangements. Alongside these technical changes, it aimed to strengthen governance, business continuity planning and technology management, embedding cyber security more consistently across the organisation.

Phased restoration and long-tail recovery

The first significant milestone in recovery was reached on 15 January 2024, when a searchable version of the main catalogue returned online in a limited, read-only format.

Service restoration then progressed in phases throughout 2024, with functionality gradually returning. The focus shifted from temporary workarounds to rebuilding core digital services on a more resilient footing. In August 2024, the Library issued a £400,000 tender as part of its Web Foundations project to support this transition.

By the second anniversary of the attack, in October 2025, recovery remained ongoing and had extended beyond the originally planned timeframe. While much of the core infrastructure had been rebuilt, some digital services remained unavailable or only partially restored, including access to e-resources, subscription databases and EThOS (E-Theses Online Service).

In a November 2025 update, the Library confirmed that recovery was still in progress, with further services scheduled for phased return. A major step followed on 15 December 2025 with the launch of a new main catalogue and an interim Archives and Manuscripts Catalogue. In January 2026, Interim Chief Executive Jeremy Silver said the Library was "starting to turn a corner", with most remaining services expected to return during 2026.

Key resilience lessons

The British Library attack is a warning for all public institutions and especially the GLAM sector. It demonstrates the risks of relying on "security through obscurity" – the assumption that cultural organisations are unlikely targets.

The reality is that they are increasingly in the crosshairs of attackers, who see them as soft targets holding valuable data, with limited cyber security budgets and ageing infrastructure.

For the GLAM sector, custodial responsibility now extends beyond the physical collection to the data and infrastructure that make it accessible. This raises a broader question: whether key cultural and knowledge institutions should be treated as part of the UK's Critical National Infrastructure (CNI), with higher standards for security and resilience.

What is clear is that there is much for other organisations to learn from the attack.

Imperative 1: Close gaps in identity and access control

The most likely entry point in the British Library attack was a remote access system without multi-factor authentication. This was a known risk. The Library acknowledged that "the possible consequences were perhaps under-appraised", and the gap remained unaddressed.

This highlights the disproportionate impact of basic control failures. The cost of implementing MFA across relevant systems would have been marginal compared to the estimated £7 million recovery cost.

Organisations should:

- Enforce multi-factor authentication across all access points, including legacy and on-premise systems
- Apply least privilege consistently, particularly for administrative and third-party accounts
- Monitor for abnormal access and privilege escalation
- Remove or restrict standing privileged access wherever possible

Imperative 2: Actively manage legacy technology risk

The Library concluded that its reliance on legacy infrastructure was "the primary contributor" to the severity of the impact.

Legacy infrastructure is not only harder to secure – it is significantly harder to recover.

Organisations should:

- Maintain a clear inventory of legacy systems and associated risks
- Prioritise replacement of systems that cannot be secured or restored
- Align lifecycle investment with both security and recovery requirements
- Avoid extending the life of unsupported or incompatible systems

Imperative 3: Design systems to limit the impact of breach

The Library's interconnected environment allowed attackers to move across systems and access large volumes of data, causing more damage than would have been possible with a modern network topology.

A key principle is to assume breach and design to contain it.

Organisations should:

- Implement network segmentation to isolate critical systems
- Apply a defence-in-depth approach across infrastructure
- Limit lateral movement through access controls and monitoring
- Reduce unnecessary duplication of sensitive data across systems

Imperative 4: Prioritise recovery capability alongside prevention

When a breach is successful, the outcome is determined by an organisation's ability to recover. In the British Library's case, the destruction of its infrastructure made the only feasible option a costly and time-consuming rebuild.

This reinforces the need for a right-of-breach mindset, where investment in recovery capability is treated as equally important as investment in protection.

Organisations should:

- Build cyber resilience by maintaining air-gapped and immutable backups
- Regularly validate backups and recovery processes
- Ensure infrastructure can support rapid restoration
- Design recovery for worst-case scenarios, including full system loss

Imperative 5: Plan to operate in a degraded state

For weeks, the Library operated using manual processes, with staff effectively replacing system functions by hand.

This level of disruption is not exceptional in a major cyber incident. Organisations must assume that critical systems will be unavailable for an extended period and plan for how they will operate in a degraded state.

Organisations should:

- Define minimum viable operations for critical services
- Establish and document manual fallback processes
- Train staff to operate without core systems

Imperative 6: Test and exercise response and recovery plans

The Library's review highlights the importance of regular, structured exercising, including for scenarios involving the "total outage of all systems", not just individual services.

Organisations should:

- Regularly test incident response and recovery plans under realistic conditions
- Exercise scenarios involving total system outage and data compromise
- Validate decision-making, coordination and communication under pressure
- Continuously refine plans based on lessons learned

Imperative 7: Use recovery to drive structural improvement

For all the damage they cause, major incidents can present opportunities. One that must be seized is the chance to use recovery as a catalyst for positive change.

The British Library made this a priority through its Rebuild & Renew programme, using recovery not simply to restore services, but to address underlying weaknesses in its technology, architecture and governance.

Organisations should:

- Rebuild systems with security and resilience embedded by design
- Introduce segmentation, stronger identity controls and improved access management
- Update governance, business continuity and risk management processes
- Align technology strategy with long-term resilience objectives

Imperative 8: Help build collective resilience by sharing insights

Detailed accounts of cyber attacks are rare because the default position for most organisations is to disclose as little as possible.

The British Library took a different approach, publishing an in-depth account of the incident, including its own shortcomings. This level of openness is valuable because it turns abstract discussions around cyber risk into real-world lessons that organisations can act on.

Organisations should:

- Participate in sector-wide threat intelligence sharing
- Share incident insights and lessons learned where possible
- Contribute to improving collective resilience

Sources

Primary source: British Library (2024) – Cyber Incident Review, 8 March 2024

Other sources: National Cyber Security Centre (NCSC), Information Commissioner's Office (ICO), BBC News, Financial Times, The Times, The Guardian, The Standard, The Independent, US Cybersecurity and Infrastructure Security Agency (CISA), IT Pro, TechRadar, Bleeping Computer, Trend Micro

Databarracks
1 Bridges Court
London, SW11 3BB

0800 033 6633
contact@databarracks.com
www.databarracks.com

Databarracks

Databarracks