LEARNING LESSONS FROM THE CYBER-ATTACK

British Library cyber incident review

8 MARCH 2024

CONTENTS

This paper aims to provide an overview of the cyber-attack on the British Library that took place in October 2023 and examines its implications for the Library's operations, future infrastructure, risk assessment and lessons learned. Its purpose is to ensure a common level of understanding of key factors that may help peer institutions and other organisations learn lessons from the Library's experience.

The report is structured as six sections, with an Executive Summary:

EXECUTIVE SUMMARY

This paper provides an overview of the cyber-attack on the British Library that took place in October 2023 and examines its implications for the Library's operations, future infrastructure, risk assessment and lessons learned.

Following an extensive forensic investigation by the Library and our cyber security specialists, this paper sets out a detailed timeline of when and how the attack took place, including a suspected instance of hostile reconnaissance a few days before the major ransomware attack of Saturday 28 October. Although the attackers encrypted or destroyed much of our server estate during the course of the attack, we have identified a server we consider likely to have been the point of entry, and explore why our security measures were not sufficient, in spite of the routine use of security assessments including penetration tests where appropriate.

The criminal gang responsible for the attack copied and exfiltrated (illegally removed) some 600GB of files, including personal data of Library users and staff. When it became clear that no ransom would be paid, this data was put up for auction and subsequently dumped on the dark web. Our Corporate Information Management Unit is conducting a detailed review of the material included in the data-dump, and where sensitive material is identified they are contacting the individuals affected with advice and support.

As well as the exfiltration of data for ransom, the attackers' methods included the encryption of data and systems, and the destruction of some servers to inhibit system recovery and to cover their tracks. The latter has had the most damaging impact on the Library: while we have secure copies of all our digital collections – both born-digital and digitised content, and the metadata that describes it – we have been hampered by the lack of viable infrastructure on which to restore it. The re-build of our infrastructure, on equipment approved and purchased before the attack, has been under way since December 2023 and remains ongoing.

The impact on the Library's systems and services has therefore been deep and extensive. Although Library premises have remained open throughout and exhibitions, events and Reading Room access have all been maintained, our research services were severely restricted in the first two months, and remain incomplete even following the return of a searchable version of our online catalogue on 15 January 2024. Staff across the Library are working hard on full restoration and are continuing to share updates with our users.

Our major software systems cannot be brought back in their pre-attack form, either because they are no longer supported by the vendor or because they will not function on the new secure infrastructure that is currently being rolled out. This includes our main library services platform, which supports services ranging from cataloguing and ingest of non-print legal deposit (NPLD) material to collection access and inter-library loan. Other systems will require modification or migration to more recent software versions before they can be restored in the new infrastructure. Our cloud-based systems, including finance and payroll, have functioned normally throughout the incident.

The paper outlines the impact of the attack on the delivery of the Library's mission and its public purposes. Most severely hit during the crisis have been our purposes relating to Custodianship and Research, as these have been directly impacted by the loss of core systems relating to collection access. Our public purposes relating to Business, Culture, Learning and International partnership have been relatively less affected, with on-site services and activities continuing largely without significant interruption, as have our partnership networks with public libraries. Exhibitions and on-site cultural events have exceeded their targets during the period.

The Library's crisis response is described and assessed, with staff engagement and internal communications highlighted as critically important. Leadership and communication took place via a range of channels throughout a highly disrupted situation, although the need to tightly control information during the early stages of the cyber-attack, and the uncertainties around the resumption of normal services, have caused frustration for researchers and had an impact on staff morale.

In December 2023, the Library began the transition from crisis response to recovery with the inception of a Rebuild & Renew programme, which will enable the restoration of services and the complete renewal of our technological infrastructure, in order to build back a more secure, resilient and innovative British Library. In parallel with the programme to modernise its library service, which was already underway, and an accelerated programme for renewing the technology infrastructure, Renew & Rebuild will align fully with the Library's *Knowledge Matters* strategy that was launched last year.

The paper considers the attack in the context of the Library's historic technology infrastructure. The Library's unusually diverse and complex technology estate, including many legacy systems, has roots in its origins as the merger of many different collections, organisational cultures and functions. We believe that the nature of this legacy infrastructure contributed to the severity of the impact of the attack. The historically complex shape of the network allowed the attackers wider access than would have been possible in a more modern network design, and the reliance of older applications on manual processes to pass data from one system to another increased the volume of staff and customer data held in multiple copies on the network.

Previously approved investment updates and changes are already being implemented that will reduce the impact of a future attack, reduce operating overheads by replacing legacy systems, embed security across the IT lifecycle and reduce risk in key areas such as data loss, disaster recovery and business continuity. Implementation will require significant changes to our applications, our culture and ways of working, and our policies and processes.

Future risk assessments must take into account the increased risk of major attacks on the Library and the significant culture change needed to fully embed cyber security at the heart of technology rebuild and all processes going forward. The challenge of rebuilding our technology infrastructure in full also brings risks of capacity and capability within our Technology department, which will need to be actively addressed. Due to the complexity of restoring, modifying, consolidating, retiring, rebuilding or replacing a large number of systems at the same time there will need to be a careful balance of informed analysis, visionary design, and firm objective setting and management.

We expect the balance between cloud-based and onsite technologies to shift substantially towards the former in the next 18 months, which will come with its own risks that need to be actively managed, even as we substantially reduce security and other risks by making this change.
Finally, the paper aims to ensure a common level of understanding of key factors that may help libraries, peer institutions and other organisations to learn lessons from the British Library's experiences since the attackers first struck. To this end, we also append a list of lessons we have learned on our own account, including some that may have wider relevance to our peers and partners.

SECTION ONE:
CAUSALITY – UNDERSTANDING THE ATTACK

CONTEXT

On Saturday 28 October 2023 it became clear that the British Library had been affected by a significant ransomware cyber-attack that compromised the majority of the Library's online systems. The attack, which was claimed by the Rhysida ransomware gang, exfiltrated data, encrypted or destroyed substantial portions of our server estate, and forcibly locked out all users from our network.

The intrusion was first identified as a major incident at 07:35 on 28 October 2023 when a member of the Technology Team was unable to access the Library's network. Initial escalation and investigation of the incident within the Technology Team as per the Technology Major Incident Management Plan confirmed the likelihood that the incident was the result of a cyber-attack; and at 09:15 the Library's Crisis Management Plan was invoked by the Business Continuity Manager. The Accounting Officer and Chief Officers were contacted and informed of the incident by 09:21 and the Gold Crisis Response Team subsequently notified, convening at 10:00 by WhatsApp video call in the absence of email.

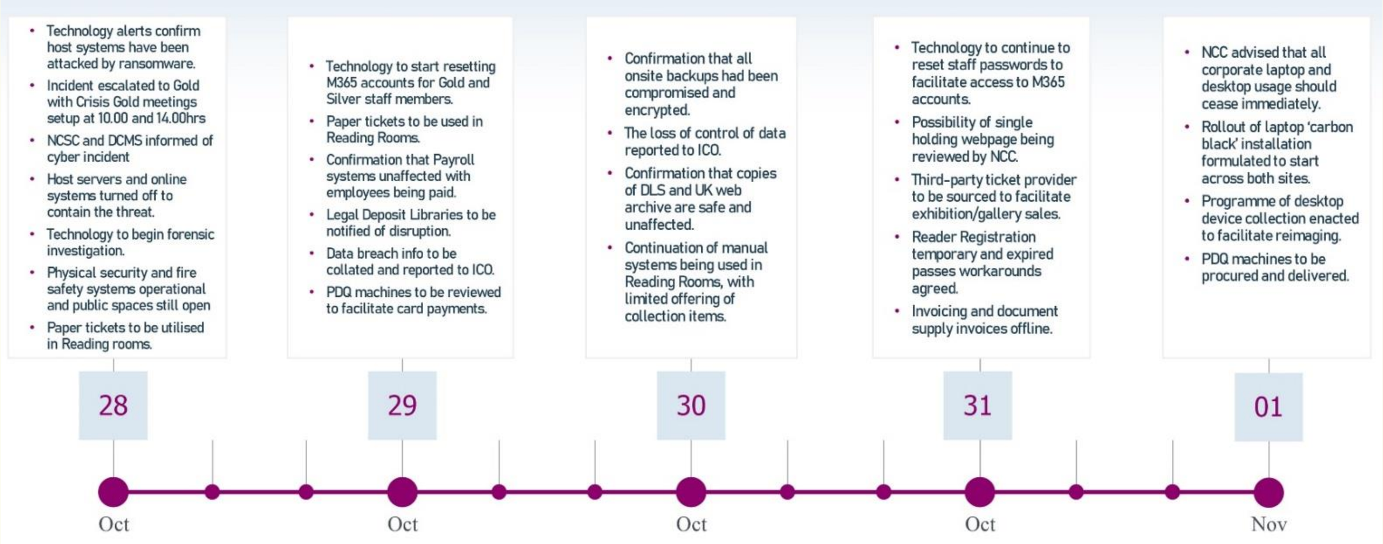
Following consultation with the National Cyber Security Centre (NCSC), specialist cyber security advisers NCC Group were procured immediately to support the Library in managing its response process. NCSC attended a subsequent Gold meeting at 14.00 on 28 October and provided early advice on incident handling, including communications strategy. Our sponsor body, the Department for Culture, Media and Sport (DCMS) and the British Library Board were informed of the situation.

The Information Commissioner's Office (ICO) and other relevant regulatory and law enforcement bodies were all contacted at appropriate points, and within the relevant statutory timeframes by our statutory Data Protection Officer & Head of Corporate Information Management. The Library has been actively cooperating with ICO's investigation of the incident from the outset and been providing regular updates and responses to questions, particularly pertaining to the loss of personal data. It is understood that the ICO will publish its own findings on the incident in due course, and the Library will abide by the recommendations of that report.

The Library has also proactively communicated with both users and staff about the disclosure of their personal data within relevant statutory deadlines, and has been providing NCSC advice as to how those affected should protect their data. On the assumption that staff personal data was likely to have been compromised, we also immediately purchased a credit monitoring and identity protection product for all staff including some ex-staff, Board members and users, if appropriate, to provide the maximum possible protection of their personal finances.

Our specialist advisers carried out a thorough analysis of the attack and delivered a report of their findings which was discussed by the Board on 21 November 2023.

The detailed timeline for the escalation process and key actions taken across the first 5 days of the incident are summarised below:



28 Oct

- Technology alerts confirm host systems have been attacked by ransomware.
- Incident escalated to Gold with Crisis Gold meetings setup at 10.00 and 14.00hrs
- NCSC and DCMS informed of cyber incident
- Host servers and online systems turned off to contain the threat.
- Technology to begin forensic investigation.
- Physical security and fire safety systems operational and public spaces still open
- Paper tickets to be utilised in Reading rooms.

29 Oct

- Technology to start resetting M365 accounts for Gold and Silver staff members.
- Paper tickets to be used in Reading Rooms.
- Confirmation that Payroll systems unaffected with employees being paid.
- Legal Deposit Libraries to be notified of disruption.
- Data breach info to be collated and reported to ICO.
- PDQ machines to be reviewed to facilitate card payments.

30 Oct

- Confirmation that all onsite backups had been compromised and encrypted.
- The loss of control of data reported to ICO.
- Confirmation that copies of DLS and UK web archive are safe and unaffected.
- Continuation of manual systems being used in Reading Rooms, with limited offering of collection items.

31 Oct

- Technology to continue to reset staff passwords to facilitate access to M365 accounts.
- Possibility of single holding webpage being reviewed by NCC.
- Third-party ticket provider to be sourced to facilitate exhibition/gallery sales.
- Reader Registration temporary and expired passes workarounds agreed.
- Invoicing and document supply invoices offline.

01 Nov

- NCC advised that all corporate laptop and desktop usage should cease immediately.
- Rollout of laptop 'carbon black' installation formulated to start across both sites.
- Programme of desktop device collection enacted to facilitate reimaging.
- PDQ machines to be procured and delivered.

<u>When was entry gained?</u>

Because of the overtly destructive nature of the attack, it is unlikely that a definitive answer will ever be gained on the exact timing of Rhysida's entry into the Library's estate. However, forensic investigation and analysis of records indicates the strong likelihood that the criminal actors initially gained access at least three days before the incident became apparent.

Forensic analysis of the attack performed by our independent cyber-security advisors has identified evidence of an external presence on the Library network at 23:29 on Wednesday 25 October 2023, with the first evidence of movement around the network at 23:32. Later that night, at 01:15 on 26 October 2023, the Library's IT Security Manager was alerted to possible malicious activity on the Library network. This alert came from the Library's Monitoring System which had automatically blocked the suspect activity at 00:21. The IT Security Manager, among other actions, extended the automatic block beyond the pre-set expiry, undertook a vulnerability scan (which came back with no results) and actively monitored activity log. No repeat activity was seen. The incident was escalated to the IT Infrastructure team at 07:00. Further investigation by the IT Infrastructure Team, including detailed analysis of activity logs, did not identify any obviously malicious activity and they subsequently performed a password reset before unblocking the account later that day.

In hindsight, the Library and its advisors believe this initial intrusion to have been hostile reconnaissance of our network, as a precursor to the major attack.

When alerted by the Library following discovery of the attack, Jisc (who provide the Library's internet access and monitor movement of data across their networks) identified that an unusually high volume of data traffic (440GB) had left the Library's estate at 1.30am on 28 October. This can now be equated with the tranche of data illegally exfiltrated by the attackers (see 'Copying and Compromising of data' below).

How was entry gained?

The investigation by our specialist cyber security advisers concluded that it is not possible to be certain of the exact point of entry to the Library's network, due to both the severe damage caused to our server estate by the attack and anti-forensic measures taken by the attackers.

However, the first detected unauthorised access to our network was identified at the Terminal Services server. This terminal server had been installed in February 2020 to facilitate efficient access for trusted external partners and internal IT administrators, as a replacement for the previous remote access system, which had been assessed as being insufficiently secure. Remote usage expanded during the subsequent Covid-19 pandemic because of the greatly increased requirement for remote working and the range of IT projects being undertaken with third party support.

The Library utilises numerous trusted partners for software development, IT maintenance, and other forms of consultancy, and whose staff have a variety of levels of access to our network or infrastructure dependent on their contract with us and the level of supervision or vetting that is undertaken. These levels of access range from supervised physical access to network components, guest access to individual sites or folders, possession of a British Library IT account and user profile for the duration of their work with us, and in many cases privileged administrator access to specific servers or software. The most likely source of the attack is therefore the compromise of privileged account credentials, possibly via a phishing or spear-phishing attack or a brute force attack where passwords are repeatedly tried against a user's account.

The increasing use of third-party providers within our network, some of which has been due to capacity and capability constraints within Technology and elsewhere in the Library, was noted by the Library's Corporate Information Governance Group (CIGG) in late 2022, and the increasing complexity of managing their access was flagged as a risk. A review of security provisions relating to the management of third parties was planned for 2024; and the tightening of access provisions that would be enabled by improvements to underlying computer and storage infrastructure and the migration of storage to the cloud, which is currently being implemented. Unfortunately, the attack occurred before these necessary pre-requisites for this work were completed.

In common with other on-premise servers, this terminal server was protected by firewalls and virus software, but access was not subject to Multi-Factor Authentication (MFA). MFA was introduced across the Library in 2020 to increase protection of all remote activities relating to cloud applications such as email, Teams and Word, but for reasons of practicality, cost and impact on ongoing Library programmes, it was decided at this time that connectivity to the British Library domain (including machine log-on access and access to on-premise servers) would be out of scope for MFA implementation, pending further renewal of the Library's infrastructure. The lack of MFA on the domain was identified and raised as a risk at this time, but the possible consequences were perhaps under-appraised. In mitigation of this risk, it was noted that all Library domain services, including this terminal server, were subject to routine security assessments, and additional measures were implemented on the server to mitigate risk including copy/paste prevention and hardening of security settings to recognised Centre for Internet Security (CIS) standards. The Library also undertakes security assessments including penetration tests where appropriate.

It is considered likely that the absence of MFA contributed to the attackers' ability to enter the system via this route, although as stated above, the exact point and method of entry cannot be stated with certainty.

While the Library's monitoring software did not automatically isolate the intrusion at source, it did intervene in some of the actions and prevented further intrusion into parts of the Library's technology estate. A different software system successfully identified and prevented the encryption attack from executing on our laptop and desktop estates, but older defensive software on the server estate was unable to resist the attack. This is being replaced in the new infrastructure currently being rolled out.

Copying and compromising of data

As a ransomware gang, the attackers' goal appears to have been the copying and removal of personal or sensitive data which has the potential to be monetised either by payment of a ransom by the affected organisation or by sale on the dark web. The data they copied amounts to some 600GB of files, which in real terms equates to just under half a million individual documents. Detailed analysis of this data is ongoing, which is estimated to be complete by the end of March 2024.

Based on analysis from our cyber security advisers, we believe the attackers used three methods of attack to identify and copy these documents.

Firstly, a targeted attack copied records belonging to our Finance, Technology, and People teams on a 'wholesale' basis, resulting in the copying of entire sections of our network drives. These files represent around 60% of the content copied in the attack.

Secondly, a keyword attack scanned our network for any file or folder that used certain sensitive keywords in its naming convention, such as 'passport' or 'confidential', and copied files not just from our corporate networks but also from drives used by staff for personal purposes as permitted under the Library's Acceptable Use of IT Policy. This policy, and the staff education that accompanies it, will be reviewed in the light of lessons learned from the cyber-attack. The files and folders copied in this way represent around 40% of the copied documents.

Thirdly, the attackers hijacked native utilities (e.g. IT tools used to administer the network) and used them to forcibly create backup copies of 22 of our databases, which were then subsequently exfiltrated from our network. We believe that several of these databases contain some contact details of external users and customers, although we will be unable to analyse exactly what data was copied in this way until some of our database infrastructure capabilities are restored. However, we do know that the customer databases compromised in this way are not full copies of our Customer Relationship Management and Single Customer View databases, but rather are extracts used for the purpose of market segmentation and the creation of email marketing lists. As such, although they are likely to contain contact details, they are not believed to contain more sensitive details such as customer bank details.

Work is now under way by our Corporate Management Information Unit to conduct a detailed review of the exfiltrated data to confirm our assumptions about the nature of its contents and identify any specific sensitive material. Where sensitive material is detected in the course of this review the individuals affected (whether staff or external) are being contacted and provided with appropriate advice or support, and the ICO is being kept informed.

We believe that the unedited Electoral Roll database held as part of the collection was not compromised, as all indications are that the enhanced levels of encryption in place on that particular database functioned as intended and protected it from the attack method described above. Similarly, our PCI DSS controls have ensured that no credit card data was compromised; the storage of customer card data is not permitted anywhere on our network and is regularly scanned for and eliminated where present.

As regards the Library's digital collection holdings, we believe that secure copies exist both of our born-digital and digitised content, and of the metadata which describes it. Each dataset will need to be validated to ensure its integrity before being restored on the Library's new infrastructure.

Encryption and destruction of infrastructure

The attack methodology of Rhysida and its affiliates involves several different elements, including defence evasion and anti-forensics (e.g. they 'clean up after themselves' and delete log files etc., in order to make it hard to trace their activities), exfiltration of data for ransom, encryption for impact, and destruction of servers to inhibit system recovery (and as a further anti-forensic measure).

It is this last attack type that has had the most damaging impact on the Library: whilst we believe that we will eventually be able to restore all of our data, we are hampered temporarily by the lack of viable infrastructure on which to restore it. This infrastructure is in the process of being rebuilt or renewed, with work due to complete by mid-April, prior to the phased restoration of systems and data. The Library's vulnerability to this particular kind of attack has been exacerbated by our reliance on a significant number of ageing legacy applications which are now, in most cases, unable to be restored, due to a combination of factors including technical obsolescence, lack of vendor support, or the inability of the system to operate in a modern secure environment. (See Section Four, below.)

Ransom payment

The Library has not made any payment to the criminal actors responsible for the attack, nor engaged with them in any way. Ransomware gangs contemplating future attacks such as this on publicly-funded institutions should be aware that the UK's national policy, articulated by NCSC, is unambiguously clear that no such payments should be made.

SECTION TWO: IMPACT

Impact on systems and services

For the reasons described above, the impact of the cyber-attack has been deep and extensive across all areas of Library activity, with users, staff and key stakeholders almost all affected to a greater or lesser extent. Library premises have remained open throughout and exhibitions, events and Reading Room access have all been maintained, but the services on offer were severely restricted in the first two months, and remain incomplete even following the launch of a searchable version of our main catalogue on 15 January. Many staff have been unable to perform significant parts of their roles or, where they have, have been required to follow more onerous manual processes in order to do so. Key externally-funded partnerships that rely on constant collection access have been substantially affected.

A few key software systems, including the library management system, cannot be brought back in the form that they existed in before the attack, either because they are no longer supported by the vendor and the software is no longer available, or because they will not function on the Library's new secure infrastructure which is in the process of being rolled out. Other systems will either require modification or migration to more recent software versions before they can be restored on the Library's new infrastructure. Our core email, finance, HR and payroll systems are cloud-based and are functioning normally, having been largely unaffected by the attack, as are our security systems, which have enabled us to keep our buildings open to the public throughout the incident.

In December, it was confirmed that viable sources of backups had been identified that were unaffected by the cyber-attack and from which the Library's digital and digitised collections, collection metadata and other corporate data could be recovered. Other data held locally on desktop PCs and other drives is currently being validated as part of the process to re-install it on the new secure infrastructure.

Calculating the cost

The process of calculating the net financial impact of the attack is ongoing. Prior to the attack, as part of its preparation for the new *Knowledge Matters* strategy (2023-2030) the British Library Board had set aside funds to cover investment in a new cyber secure infrastructure as well as legacy systems replacement and knowledge management technology. A significant proportion of this spend will now be brought forward, and a revised 3-year budget, incorporating any additional IT costs and lost income attributable to the attack, will be brought for approval by the Board later in the year. It is Library policy to hold an unrestricted reserve at all times which is designed to help it navigate unexpected incidents. We have not at this point approached DCMS for additional funds.

Impact on Library's delivery of its purposes

Since 2015 the Library has reported its overall performance annually against a framework of six statements of purpose, which together with its overall mission statement set out the distinctive types of public value which the institution delivers. This section summarises the qualitative impact of the attack on the delivery of each of our purposes over the period of the incident so far.

CUSTODIANSHIP – *WE BUILD, CURATE AND PRESERVE THE UK'S NATIONAL COLLECTION OF PUBLISHED, WRITTEN AND DIGITAL CONTENT* *RED / AMBER*

- Physical collections largely unaffected in terms of security and preservation, though some issues with real-time environment monitoring (workarounds are in place)
- Digital collections all accounted for through back-ups and/or third-party copies, though final full validation will only be possible once each dataset is checked and brought back on stream on the new infrastructure
- Access to collections for staff is still limited, with knock-on effects across multiple Library functions
- Print legal deposit continues to be received but cannot currently be accessioned or sent to shelf
- Ingest of non-print legal deposit (NPLD) not currently available
- Physical conservation and disaster preparedness remain possible with workarounds
- Loans to other institutions continuing, with some restrictions
- Terms of NHLF-funded Unlocking our Sound Heritage grant not currently being met through lack of access to website
- Digitisation activity currently paused, affecting partnership projects and commercial income.

RESEARCH – *WE SUPPORT AND STIMULATE RESEARCH OF ALL KINDS* *RED / AMBER*

- Significant disruption and frustration caused to researchers who are reliant on unique British Library content
- Reading Rooms have remained open, but access to physical collection remains limited to c50% of total by volume. Content held in Boston Spa automated vaults currently not accessible
- Majority of St Pancras physical holdings now useable, including the most commonly used and rarest items
- Searchable version of main catalogue available online since 15 January, covering the content that can be ordered onsite using manual processes
- Research access not currently available to: e-resources, NPLD (including via Legal Deposit Library partners), online journals, databases, EthOS (online theses), audio/video and other digital content
- Enquiries system and chat not currently available although staff supports users via email, telephone and in person
- British Library On Demand has resumed with a targeted service focussed on health, higher education and law sectors.

BUSINESS – *WE HELP BUSINESSES TO INNOVATE AND GROW* *GREEN / AMBER*

- Business support services in London and across Business & IP Centre (BIPC) National Network have continued, with quarterly and annual targets being exceeded
- 8000 attendees to on-site or online workshops during Q3 (47% above target)
- No access to databases at St Pancras but availability provided through partner BIPCs in London and nationally
- Lack of website restricting ability to market and raise future funding.

CULTURE – *WE ENGAGE EVERYONE WITH MEMORABLE CULTURAL EXPERIENCES* *GREEN*

- All activities and events have continued, with workaround; successful performance in spite of cyber-attack.
- *Fantasy: Realms of Imagination* concluded its run at 105% of target – most successful exhibition since the Covid-19 pandemic
- *Malorie Blackman: The Power of Stories* at 114% of target, very popular with schools
- Treasures Gallery also well ahead of target: 352k to date vs target of 284k
- Events ahead of target: 39k sales vs target 33k

- Living Knowledge Network website unaffected by the cyber-attack. Panel version of *Fantasy* currently on display in 78 public libraries, set to reach/exceed 650k footfall target
- Some risk to future exhibition programme through current restriction on access to collection.

LEARNING – *WE INSPIRE YOUNG PEOPLE AND LEARNERS OF ALL AGES* *GREEN / AMBER*

- On-site activity in London and Leeds has continued successfully with minor workarounds
- Targets exceeded – 6000 students participants since cyber-attack, including popular workshops for *Fantasy* and *Malorie Blackman*
- On-site adult courses, programmes for people with complex or profound needs, weekly Family Station, storytelling for under 5s have all continued strongly
- By contrast, online Learning delivery via the popular *Discovering…* sites has been effectively paused since the attack, with the loss of the website
- Launch of the externally-funded *Discovering Historical Sources* website has been delayed.

INTERNATIONAL – *WE WORK WITH PARTNERS AROUND THE WORLD TO ADVANCE KNOWLEDGE AND MUTUAL UNDERSTANDING* *GREEN / AMBER*

- International engagements have continued largely unimpeded through Quarter 3: 23 diplomatic visits, 89 professional engagements
- Successful call issued for applicants to 2024 Library Leaders Programme
- Touring exhibition *Luminous* (Hebrew Manuscripts) with 37 loan items has gone ahead successfully in State Library Victoria, Australia
- Risk to Qatar Foundation partnership programme through delay to activity – timetable for recovery currently being prioritised
- Temporary delay to new International Dunhuang Project website, but successfully launched in February 2024
- Endangered Archives Programme (EAP) Hubs and EAP grants programme have continued well but access to previously digitised content remains currently unavailable.

SECTION THREE: CRISIS RESPONSE AND RECOVERY

Initial response

The Library immediately activated its major crisis management plans in response to the attack, convening its Gold and Silver committees to provide strategic and operational management of the incident. This Gold/Silver command structure superseded the Library's normal management structures for the duration of the crisis until the situation stabilised in mid-January. Given the wide-ranging nature of the incident the membership of these committees included senior technical staff, independent cyber-security advisors, and the Library's statutory Data Protection Officer, as well as members of senior management. The Library also received strong and consistent support from DCMS, including from their specialist cyber team, right from the beginning of the incident.

In line with our crisis management plans, the Gold/Silver command structure coordinated the Library's technical response to the attack, approved workarounds or expenditure to rapidly restore critical business processes, and coordinated all internal and external communications.

Following guidance from NCSC, the Library's Communications and Marketing teams sought to keep users, staff and stakeholders updated about what was happening without sharing detail that could aid the attackers. With the website and intranet out of action, this was initially done via the Library's social media channels and, for staff, cascaded via email or WhatsApp.

Once it was safe to do so, we actively contacted Readers, supporters, Public Lending Right (PLR) users and others on our mailing lists via email. They were signposted towards appropriate NCSC security guidance and user feedback was used to shape FAQs that were shared with public-facing staff and posted on our publicly accessible corporate blog and, subsequently, the interim website that has been in place since December. Our communications process ensured that staff always saw updated external communications (e.g. external statements, blog posts by the CEO) before the public, giving them the opportunity to digest the latest developments in advance of user queries.

Proactive engagement between management and the Library's trade unions helped to address staff concerns, and the unions also played a key role in providing grassroots-level information and advice to affected staff.

Practical operational-level lessons relating to our disaster management processes have been recorded by Gold and Silver committees throughout the incident and will be filtered back into future practice and procedures.

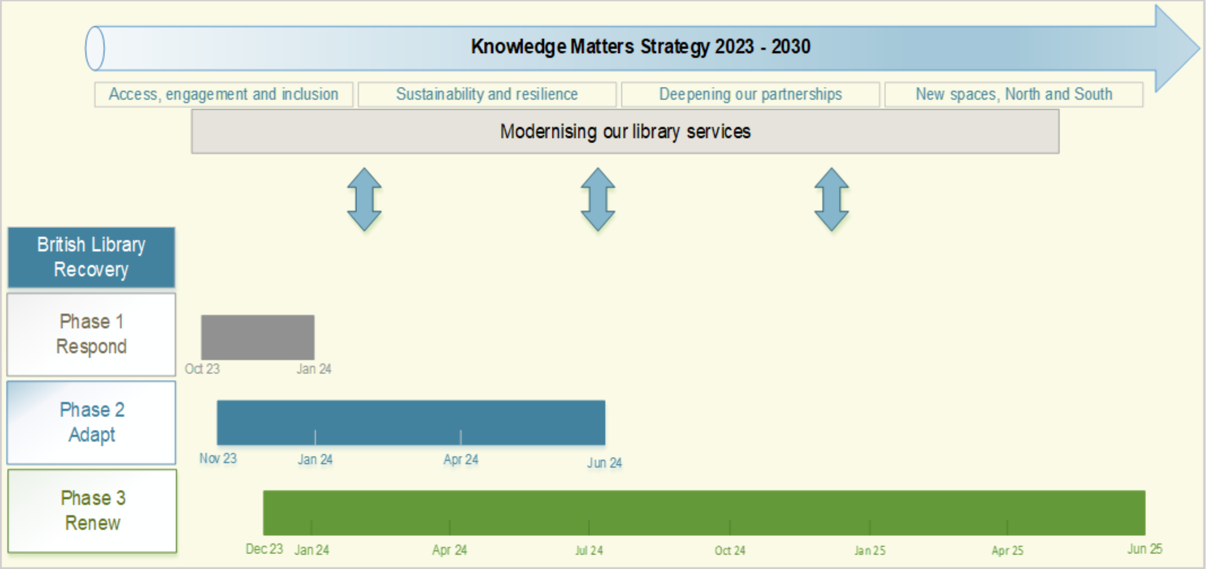
Rebuild & Renew programme

At its meeting on 20 December 2023, the British Library Board approved a proposal to establish a new Rebuild & Renew programme to plan, coordinate and deliver the Library's longer term recovery. This was to take the place of the Gold and Silver Crisis Response Teams as the immediate crisis period was considered over. This programme was to be in place for a period of 18 months and to consist of 3 distinct but concurrent phases:

Respond: Immediate crisis management phase

Adapt: 6 month phase to identify and implement interim solutions to restore services, internal processes and partnerships

Renew: 18 month phase to create a new resilient infrastructure and deliver permanent solutions, either by upgrading or adapting existing systems or delivering new ones where necessary.


Knowledge Matters Strategy 2023 - 2030
Access, engagement and inclusion
Sustainability and resilience
Deepening our partnerships
New spaces, North and South
Modernising our library services
British Library Recovery
Phase 1 Respond
Oct 23
Jan 24
Phase 2 Adapt
Nov 23
Jan 24
Apr 24
Jun 24
Phase 3 Renew
Dec 23
Jan 24
Apr 24
Jul 24
Oct 24
Jan 25
Apr 25
Jun 25

The Rebuild & Renew Programme has now been established, a Programme Board formed and a governance structure put in place. It is being overseen, alongside other digital programmes, by a new Board sub-committee, the Digital Portfolio Committee, to which external cyber expertise will be recruited.

The programme will consist of two core projects covering the Adapt and Renew phases respectively with work streams created within each to take specific initiatives forward. Within the Adapt phase, those interim solutions that can be delivered without significant input from the Technology Team and/or significant funding will be taken forward separately to those which are more complex. This is to avoid the risk of smaller initiatives becoming “lost” among the more significant changes and to ensure a consistent pipeline of improvements, however small, throughout the 6 month duration of the Adapt phase.

Other areas will be delivered as cross-cutting projects supporting the programme as a whole, with particular weight being given to Change Management. The programme will also review the Library’s corporate approach to Business Continuity, as opposed to within individual departments, incorporating lessons learned to ensure its future ability to respond to incidents of a similar scale in a consistent and structured way. Formal testing and exercise regimes will also be reviewed to enhance the Library’s overall preparedness for major incidents.

The Rebuild & Renew Programme envisions the transformation of the British Library into a more secure, resilient, and innovative institution, seizing the opportunity to build back with greater resilience in the aftermath of the cyber-attack. Emphasising a commitment to excellence and alignment with *Knowledge Matters* priorities, the programme aims to not only restore disrupted services but to strategically modernise and enhance Library operations, ensuring they remain at the forefront of delivering valuable knowledge services to our users.

Comprehensive change management will be required to build a culture of adaptability and resilience, ensuring we can effectively navigate future challenges. The objectives of this aspect of the programme will be to enable all staff to thrive and to be effective colleagues in a constantly changing, uncertain digital world.

SECTION FOUR:
TECHNOLOGY INFRASTRUCTURE

Infrastructure, Data Management and Applications

The British Library has historically had an unusually diverse and complex technology estate, with a large number of legacy systems. Formed out of the very different collections and organisational cultures brought together by the 1972 British Library Act, and with the periodic subsequent addition of other collections and organisations (most recently Public Lending Right in 2013), the Library collects and preserves websites, ebooks and ejournals under legal deposit; hosts the catalogue of the national collection, administers the Public Lending Right, digitises millions of heritage items as well as sound and video recordings. It has a commercial online and onsite shop, box office, Reader Registration system and a multitude of back office support systems, as well as an extensive security and door access network. It also has digitisation partnerships with, among others, the Qatar Foundation, Find My Past, National Life Stories, the Endangered Archives Programme and the International Dunhuang Programme.

The complexity of the Library's technology estate was increased significantly by the implementation in 2013 of the Non Print Legal Deposit Regulations, in partnership with the other five Legal Deposit libraries of the UK and Ireland. This required investment from core Library funds in a significant suite of new statutory activities including web archiving, digital preservation systems and viewing applications. One implication of this was that some legacy applications for core Library operations were retained longer than originally intended.

This has had an impact on the Library's ability to remain compliant with developing security standards. Accreditation to Cyber Essentials Plus was successfully achieved in 2019, but changes to the standard in 2022 meant that we ceased to be compliant pending replacement of some of our older core systems. Work to address this, including a major programme approved by the British Library Board in 2022 to procure and implement a new library services platform, was under way at the time of the attack. The Library was also part of the GovAssure pilot at the time of the attack.

From our investigations into the incident, we believe that the particular nature of our infrastructure contributed to the severity of the impact of the attack, in three specific ways:

- our historically complex network topology (ie. the 'shape' of our network and how its components connect to each other) allowed the attackers wider access to our network than would have been possible in a more modern network design, allowing them to compromise more systems and services
- some of our older applications rely substantially on manual extract, transform and load (ETL) processes to pass data from one system to another. This substantially increases the volume of customer and staff data in transit on the network, which in a modern data management and reporting infrastructure would be encapsulated in secure, automated end-to-end workflows
- our reliance on legacy infrastructure is the primary contributor to the length of time that the Library will require to recover from the attack. These legacy systems will in many cases need to be migrated to new versions, substantially modified, or even rebuilt from the ground up, either because they are unsupported and therefore cannot be repurchased or restored, or because they simply will not operate on modern servers or with modern security controls.

There is a clear lesson in ensuring the attack vector is reduced as much as possible by keeping infrastructure and applications current, with increased levels of lifecycle investment in technology infrastructure and security. The Library responded as quickly as it could in the circumstances, and followed the necessary steps to limit the attack, but still suffered very significant damage.

Post-Attack

Following the October 2023 attack, the Library has an opportunity to transform its use and management of technology across the organisation, to wholly adopt and embed best practice security mandates, and to implement fit for purpose policies and processes that will enable us to fully realise the benefits of our technology.

The substantial disruption of the attack creates an opportunity to implement a significant number of changes to policy, processes, and technology that will address structural issues in ways that would previously have been too disruptive to countenance.

Previously approved investment changes are already being implemented that will reduce the likelihood and impact of a future attack, reduce overheads in the administration of legacy IT infrastructure and software, eliminate technical debt, embed security across the IT lifecycle and reduce risk in key areas such as data loss, disaster recovery and business continuity. Our renewed infrastructure will have:

- a best practice network design, implementing proper segmentation with a defence in depth approach
- a hybrid compute landscape that securely leverages all the benefits of the cloud for development, application, and virtualisation
- a best practice role-based-access control setup for domain and storage services, enshrining the principle of least privilege across the organisation
- a robust and resilient backup service, providing immutable and air-gapped copies, offsite copies, and hot copies of data with multiple restoration points on a 4/3/2/1 model
- a holistic, integrated security suite that covers the whole organisation, backed by managed security partners for improved incident response, detection, and remediation
- substantially enhanced MFA on-premises capabilities
- substantially enhanced management of third party network access via Privileged Access Management (PAM)
- improvements in cyber incident, event, and vulnerability management
- a clear and defined set of policies, processes, and standard operating procedures to govern and manage the IT lifecycle, enshrining security in each phase of the IT lifecycle and unlocking efficiency and velocity gains through standardisation in Development
- compliance with mandated standards and frameworks
- stronger and more embedded governance structures to manage the rapid delivery of security enabled applications to the business.

Implementation of a modern and secure technology infrastructure will require significant changes to our applications, our culture and ways of working, and our policies and processes. In addition to the modernisation of our underlying infrastructure and technology governance, the cyber-attack – deeply unwelcome as it is – has presented the Library with an opportunity to consolidate key Library systems with modern user-centred applications running on the new infrastructure.

The main vehicle for this will be the Modern Library Services Programme which will centralise and replace our current Library Services Platform, legacy catalogues, online reader registration system, digital preservation system, and enquiries management system. Similarly, our multiple customer data systems will be consolidated into a new data management and reporting architecture, and our back-office tools and storage will be modernised and centralised, in accordance with the Knowledge & Information Management Strategy approved by the Board in 2023.

SECTION FIVE:
FUTURE RISK ASSESSMENT

More than half of the risks and actions recorded on the Library's risk registers have been impacted by the cyber-attack. Some risks have increased, either by the damage caused by the attackers, or by the inability to progress with mitigating actions. Other risks have been reduced or entirely obviated, for example by the forced retirement of ageing systems. These risks will be managed by the Library's normal risk management processes once they have been reviewed and re-baselined.

However, there are some new or substantially increased risks to the Library that are worth highlighting here:

- The Library may be at increased risk of cyber-attack going forward, because a successful cyber-attack can encourage opportunistic attackers to either take advantage of the disruption of the initial attack and rebuild phase, or to search for other flaws in the organisation's cyber security. It is therefore essential that sound cyber-security is placed and maintained at the heart of our technology rebuild activities.

- The need to embed security more deeply than ever into everything we do will require investment in culture change across different parts of the Library. There is a risk that the desire to return to 'business as usual' as fast as possible will compromise the changes in technology, policy, and culture that will be necessary to secure the Library for the future. A strong change management component in the Rebuild & Renew Programme will be essential to mitigate this risk, as will firm and well considered leadership from senior managers.

- The Technology department was overstretched before the incident and had some staff shortages which were beginning to be successfully addressed. Faced with the challenge of rebuilding our entire IT infrastructure, there is a risk that the capacity and capability within the Technology department will not be sufficient to meet the needs of the Rebuild & Renew Programme. The need to grow cyber-security capacity and cloud engineering capabilities will be particularly acute and will be difficult to remediate without reconsideration of how the Library remunerates high-demand IT skills.

- The Library is faced with the need to prioritise the restoration, modification, consolidation, retirement, rebuild or replacement of a large number of separate IT systems. There is a risk that a lack of detailed understanding of these systems and the inherent complexity of the Library's combination of services will either inhibit the pace of recovery required by the Rebuild & Renew Programme, or lead to sub-optimal decision-making. The Rebuild & Renew Programme will need a careful balance of informed analysis, visionary design, and firm objective setting and management in order to successfully navigate this risk.

- The Library's balance between cloud and on-site technologies will shift considerably over the next 18 months. There are risks and issues associated with this shift that will need to be assessed and managed, including varying levels of staff familiarity with at-scale cloud technology solutions and a whole new set of cyber-security risks. Moving to the cloud does not remove our cyber-risks, it simply transforms them to a new set of risks that should be easier to manage given the necessary resources and capacity.

SECTION SIX:
LEARNING LESSONS FROM THE ATTACK

Sector-wide Lessons

Many of the major collections institutions in the DCMS family and the wider sector are likely to have similar risks to the British Library in terms of investment levels in cyber-security, legacy infrastructure, and difficulties attracting and retaining sufficient IT talent. A significant part of the national collection, across multiple institutions, now exists in digital form – in some cases digital-only – and we all have a vital interest in ensuring that this vast and growing national asset is protected from increasingly sophisticated and destructive cyber-attacks.

Investment, boldness and relentless focus are all needed to ensure that we are as secure as we can be against this threat, as the cost of investing in prevention is outweighed by the risk of failing to prevent.

Although the security measures we had in place on 28 October 2023 were extensive and had been accredited and stress-tested, with the benefit of hindsight there is much we wish we had understood better or had prioritised differently. With that in mind, this section identifies a number of early lessons from this attack which may be helpful for others as they consider their own investments and risk management in this areas.

1. **Enhance network monitoring capabilities:** Legacy network topology may prevent modern security tools from having full coverage or from being fully effective. The Library had modern tools in place, but they were not able to completely monitor or protect our network.

2. **Retain on-call external security expertise:** Having a specialist external security advisor on retainer allows for additional resilience, improved speed of response, and depth of analysis in the earliest stages of an incident.

3. **Fully implement multi-factor authentication:** Multi-factor authentication needs to be in place on all internet-facing endpoints, regardless of any technical difficulties in doing so. The Library had MFA in place for all end-user technologies, but not on certain supplier endpoints.

4. **Enhance intrusion response processes:** An in-depth security review should be commissioned after even the smallest signs of network intrusion. It is relatively easy for an attacker to establish persistence after gaining access to a network, and thereafter evade routine security precautions.

5. **Implement network segmentation:** No perimeter can be made entirely secure. Network segmentation is therefore essential in limiting the damage caused by a successful attack. The Library's legacy network topology meant that the attack was able to cause more damage than would have been possible in a modern network design.

6. **Practice comprehensive business continuity plans:** Business continuity plans for the total outage of all systems need to be practised regularly, in addition to those relating to individual systems and services.

7. **Maintain a holistic overview of cyber-risk:** Regardless of risk appetite, all IT security risks accepted at an operational level should be flagged to the appropriate levels of senior management, to create a holistic overview of risk. The Library's risk management processes

appropriately escalated out-of-appetite security risks for remediation, but were less effective in modelling the amount of low-level risks being carried in aggregate.

8. **Manage systems lifecycles to eliminate legacy technology:** 'Legacy' systems are not just hard to maintain and secure, they are extremely hard to restore. Regular investment in the lifecycle of all critical systems – both infrastructure and applications – is essential to guarantee not just security but also organisational resilience.

9. **Prioritise remediation of issues arising from legacy technology:** The remediation of legacy issues at pace needs to be prioritised at every level in the organisation.

10. **Prioritise recovery alongside security:** Given that no security is perfect, the ability to quickly recover is essential when (not if) an attack is successful. Investment in security needs to be balanced against investment in back-up and recovery capabilities.

11. **Cyber-risk awareness and expertise at senior level:** All senior officers and Board members need to have a clear and holistic understanding of cyber-risk, in order to make optimal strategic investment choices. Current risks and mitigations should be frequently and regularly discussed at senior officer level. The recruitment of a Board member or Board-level adviser with cyber expertise is strongly recommended.

12. **Regularly train all staff in evolving risks:** All staff have a part to play in ensuring the security of the organisation. Regular training and awareness communication, covering both cyber-security basics and emerging risk trends, are essential for all staff, tailored to their role and level of expertise.

13. **Proactively manage staff and user wellbeing:** Cyber-incident management plans should include provisions for managing staff and user wellbeing. Cyber-attacks are deeply upsetting for staff whose data is compromised and whose work is disrupted, and for users whose services are interrupted.

14. Review acceptable personal use of IT: Policies and guidance on acceptable use of IT need to cover best practices for personal data security. The level of intrusion into the lives of individual staff members can be exacerbated where the use of network storage is allowed for personal use.

15. Collaborate with sector peers: Encourage collaboration and information sharing with sector peers to stay informed about common threats and best practices in cybersecurity.

16. **Implement Government standards, review and audit policies and processes regularly**: The Library was accredited Cyber Essentials Plus from 2019 until 2022, when changes to the standard meant that we ceased to be compliant pending replacement of some of our older core systems. We will continue to ensure we meet cyber security minimum standards as defined by DCMS, and our new infrastructure will be built to Cyber Essentials Plus standard in recovery.