

# Kidnapping a Library



How Ransomware Taught the British Library  
to Follow Well-Known Best Practices

# Brian Myers PhD, CISSP, CCSK



## Experience

- 20 years in software development
- 9 years in information security

## Past Positions

- Director of InfoSec, WebMD Health Services
- Senior AppSec Architect, WorkBoard
- Senior Risk Advisor, Leviathan Security

## Current Work

- Independent Information Security Consultant

# 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.

# Agenda

The British Library

The Attack

The Consequences

Lessons Learned

# The British Library



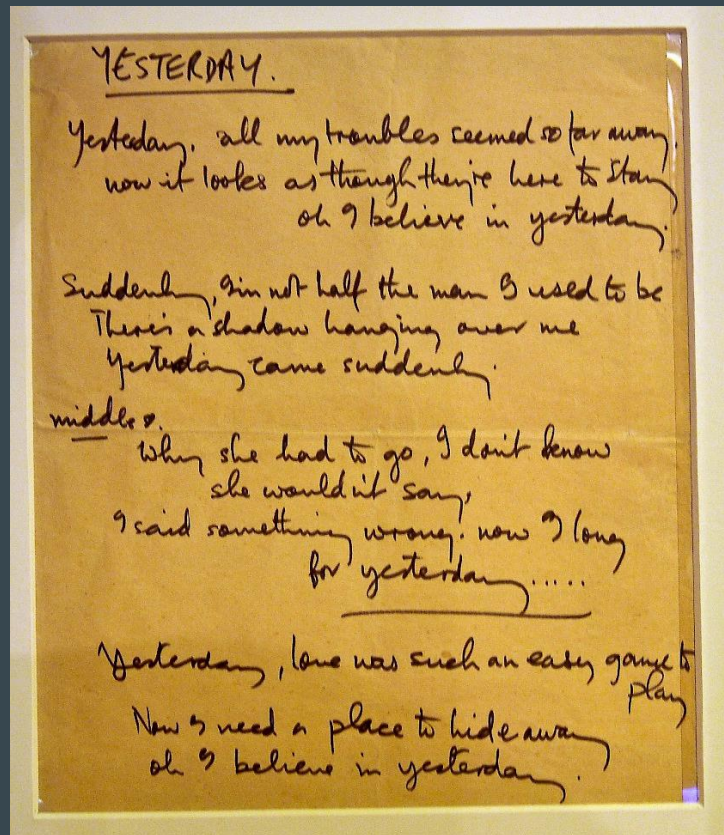
# History

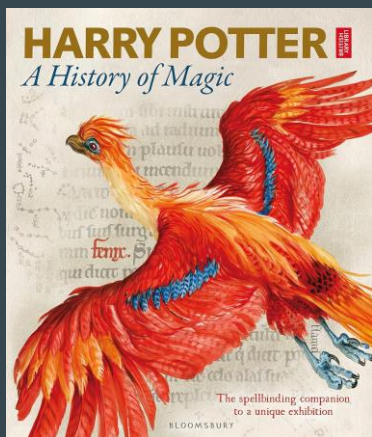
regularly acquiring  
disparate collections

1972	British Museum books
1970s	Newspaper Library Patent Office Library
1982	India Office Library
1983	National Sound Archive
2004	UK Web Archive Endangered Archives
2000s	Digitization partnerships
2013	Non-print Legal Deposit Library



# Manuscripts and Books













Bookshop

Exhibitions

Gift ideas

Shop by product

Shop by theme

Prints

Custom clothing

Christmas



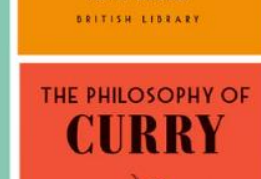
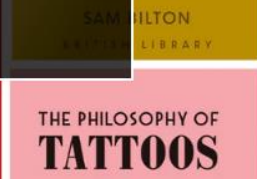
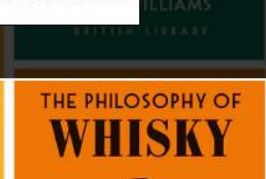
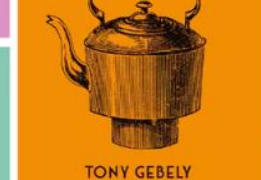
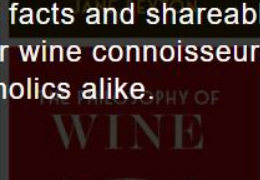
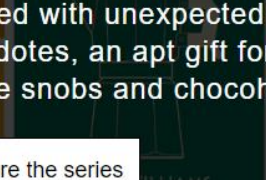
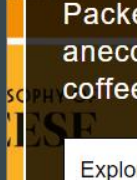
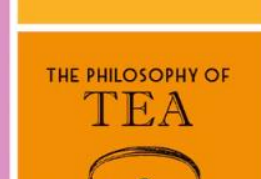
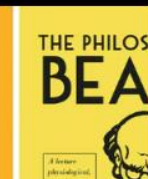
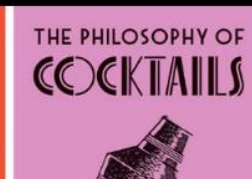
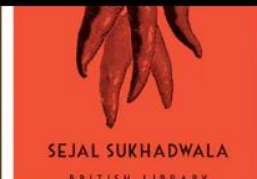
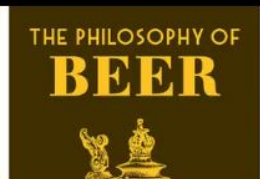
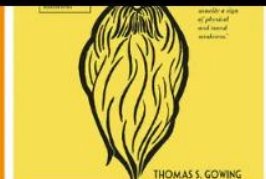
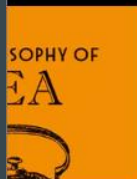
FREE UK Shipping on orders over £75 | Every purchase supports the British Library

## The Philosophy of...

Enjoy 3 for the price of 2

Packed with unexpected facts and shareable anecdotes, an apt gift for wine connoisseurs, coffee snobs and chocoholics alike.

Explore the series



## Survey, Preservation and Digitisation of Palm-leaf Manuscripts (Iontar) in Private Collections of Bali and Lombok. (EAP1241)



Inspecting manuscripts in Karangasem

# How Big is the British Library?

Printed items	170 million	
Bookshelves	466 miles	+6 per year
Web pages	1.56 petabytes	
Staff	1700 people	librarians, researchers, IT, administrative staff
Annual Budget	£142 million [\$200m]	2023



# What Information Systems Does the Library Have?

## Public-facing website

- Online learning materials
- Reader registration
- Digital archive access

## Internal network

- Firewalls, terminal servers...
- Office systems: HR, Payroll, Email, file shares...

## POS systems on site

- Cafe, gift shop

## Collections

- Digital archives
- Online catalog(s)

# What's the Library's Infosec Program Like?

Firewalls (Sophos XG)

MFA

Incident Response Plan

Risk Register

CIS hardening standards

Routine security assessments

MDM on endpoints

PCI encryption for credit card data

Business Continuity Manager

Corporate Information Governance  
Group (CIGG)

Security roadmap (plans to address  
known risks)

Regular risk assessment activity

“Cyber Essentials” assessment passed in  
2019

Recently upgraded Terminal Services  
server

# Agenda

The British Library

**The Attack**

The Consequences

Lessons Learned

# The Attack



# Rhysida's Modus Operandi

## GAIN ENTRY

- Leverage external-facing remote services  
*(such as VPNs)*
- Phish
- Authenticate with compromised valid credentials.  
*(Often lack of MFA makes this easier.)*

## LOOK AROUND

- Evade detection by “living off the land.”
- Lateral movement with built-in tools  
*ipconfig, RDP, PowerShell...*
- Steal data for double extortion

## ATTACK

- Inject ransomware into running processes
- Encrypt files, adding *.rhysida* extension
- Create a ransom note PDF with payment instructions
- Delete ransomware

*Source: CISA Cybersecurity Advisory, Nov 15 2023*




Date	Event
Oct ??	Rhysida gets credentials for a third-party account with access to BL network
Oct 25 (late Tue)	Attacker logs in through Terminal Services
Oct 26 1 AM	Automatic alert investigated; nothing found
Oct 26 7 AM	Further investigation; account re-enabled with new password

Date	Event
Oct ??	Rhysida gets credentials for a third-party account with access to BL network
Oct 25 (late Tue)	Attacker logs in through Terminal Services
Oct 26 1 AM	Automatic alert investigated; nothing found
Oct 26 7 AM	Further investigation; account re-enabled with new password
Oct 26-28	Attackers explore network: <ul style="list-style-type: none"><li>• Copy full sections of network drives</li><li>• Search across files for keywords (“passport”; “confidential”...)</li></ul>

Date	Event
Oct ??	Rhysida gets credentials for a third-party account with access to BL network
Oct 25 (late Tue)	Attacker logs in through Terminal Services
Oct 26 1 AM	Automatic alert investigated; nothing found
Oct 26 7 AM	Further investigation; account re-enabled with new password
Oct 26-28	Attackers explore network: <ul style="list-style-type: none"><li>• Copy full sections of network drives</li><li>• Search across files for keywords (“passport”; “confidential”...)</li></ul>
Oct 28 Sat 1:30 AM	440 GB of network traffic leaves the library network

Date	Event
Oct ??	Rhysida gets credentials for a third-party account with access to BL network
Oct 25 (late Tue)	Attacker logs in through Terminal Services
Oct 26 1 AM	Automatic alert investigated; nothing found
Oct 26 7 AM	Further investigation; account re-enabled with new password
Oct 26-28	Attackers explore network: <ul style="list-style-type: none"><li>• Copy full sections of network drives</li><li>• Search across files for keywords (“passport”; “confidential”...)</li></ul>
Oct 28 Sat 1:30 AM	440 GB of network traffic leaves the library network
??	Ransomware runs

Date	Event
Oct ??	Rhysida gets credentials for a third-party account with access to BL network
Oct 25 (late Tue)	Attacker logs in through Terminal Services
Oct 26 1 AM	Automatic alert investigated; nothing found
Oct 26 7 AM	Further investigation; account re-enabled with new password
Oct 26-28	Attackers explore network: <ul style="list-style-type: none"><li>• Copy full sections of network drives</li><li>• Search across files for keywords (“passport”; “confidential”...)</li></ul>
Oct 28 Sat 1:30 AM	440 GB of network traffic leaves the library network
??	Ransomware runs
7:35 AM	 <b>IT Outage.</b> Ransomware confirmed.
9:15 AM	Incident declared; crisis team in communication via WhatsApp

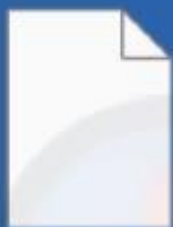




SATURDAY, 10/28/2023  
7:35 AM



CRITICAL ALERT ALERT



1.jpg.rhysida



2.png.rhysida



3.exe.rhysida



4.xlsx.rhysida



5.pptx.rhysida



6.docx.rhysida



CriticalBreach  
Detected.pdf

## Critical Breach Detected – Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen – your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network. The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets. This could inflict significant reputational and financial damage.

However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal: [rhysidafoh\[REDACTED\].onion](http://rhysidafoh[REDACTED].onion) with your secret key [REDACTED]

It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key. Together, we can restore the security of your digital environment.

# Systems Down. Business Halts.

- Reader registration
- Online catalog
- Book requests
- Access to digital assets
- Deliveries from Yorkshire
- Environmental monitoring
- Phone line
- Network access
- Wifi
- Website
- Exhibition ticket sales
- Gift shop sales

# What Exactly did the Attackers Do?

## THEFT

- Files from Finance, Tech, and HR departments
- Some personal staff files
- Included contact info for some staff, partners, and customers.

## DESTRUCTION

- Destroyed data
  - Encrypted files and backups
- “Destroyed servers”
  - Aggressively deleted logs and partitions, rendering some servers inoperable and unrecoverable.



# Agenda

The British Library

The Attack

**The Consequences**

Lessons Learned

# The Ransom

Sat Oct 28	9:15 AM - Ransomware note received (amount undisclosed)
Tue Nov 14/15	BL confirms that a ransomware attack has occurred and personal data of users and staff was stolen
Mon Nov 20	Rhysida puts 10% of stolen data up for sale (20 BTC / \$750,000)
Mon Nov 29	Rhysida dumps the remaining stolen data

*“The UK’s national policy, articulated by NCSC, is unambiguously clear that no such payments should be made [by publicly funded organisations.]”*

# Aftermath

---

Sat Oct 28	9:15 AM - Incident declared 10:00 AM - Crisis Response Team convenes on WhatsApp
Mon Oct 30	Library re-opens in “a pre-digital state” Confirmed that all onsite backups were encrypted
Wed Nov 1	All corporate desktop/laptop use ceases
Wed Nov 15	BL public states they are still determining full extent of the attack
Jan 2024	Some online catalog access restored
Mar 2024	50% of online catalog access restored

---

# British Library: Employee data leaked in cyber attack

21 November 2023

Share  Save 

CRIME

## British Library cyberattack likely to cost 40% of its financial reserves

The Library is expected to pay millions to rebuild its cyberdefences, with the repair work estimated to cost at least £6 million



British Library

@britishlibrary · [Follow](#)



We're continuing to experience a major technology outage as a result of a cyber-attack. This is affecting our website, online systems and services, as well as some onsite services. Our sites are still open and you can find details of the services available, plus other useful... [Show more](#)

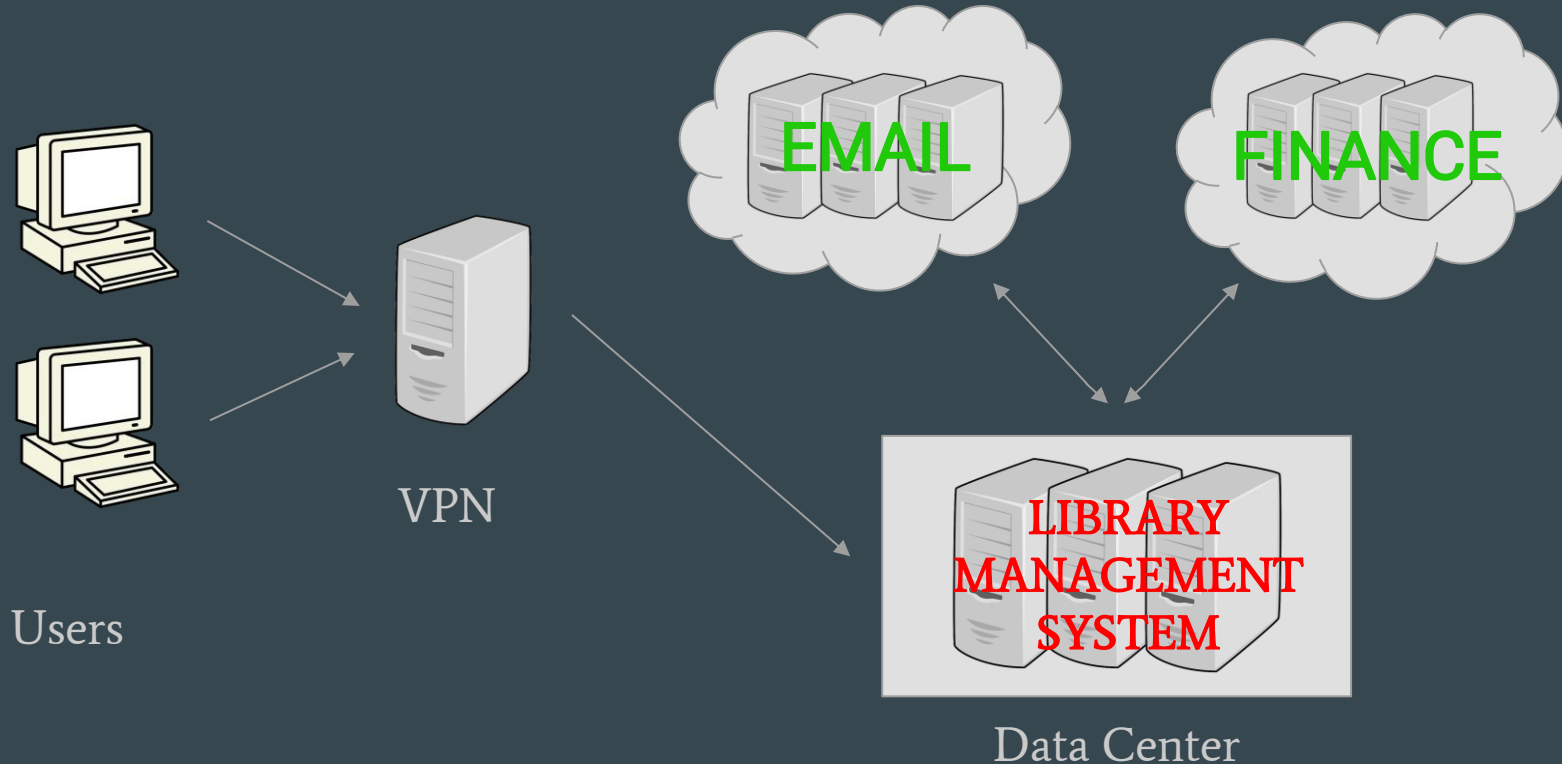
Service  
update

10:41 AM · Nov 27, 2023



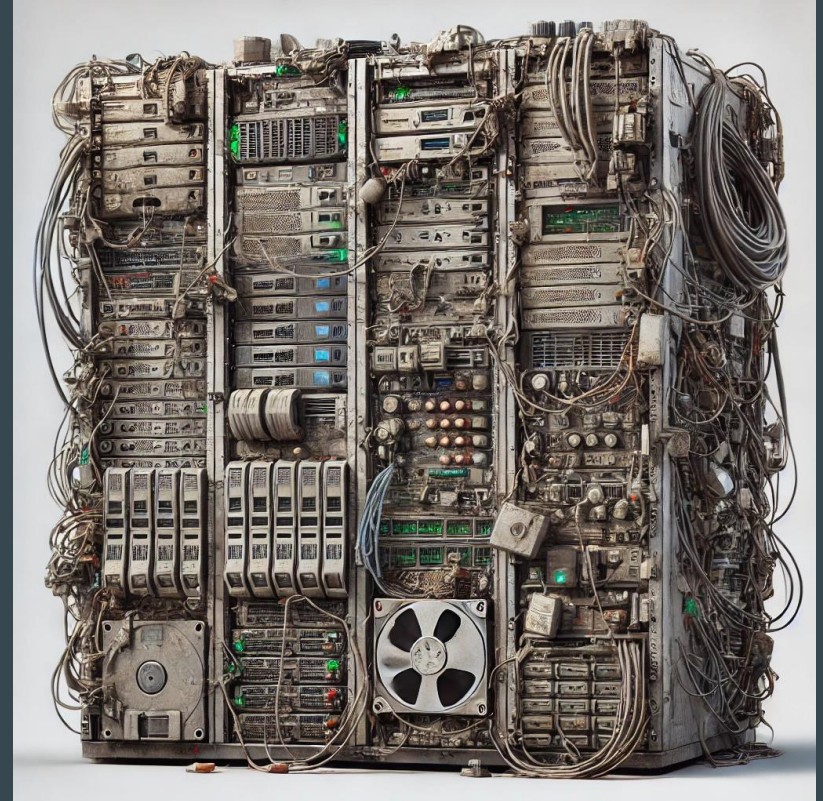
*"What we did have to think about constantly was storytelling and narrative and communication with our stakeholders, with our staff, with our board – everyone we work with in the British Library..."*

# Which Systems Were Most Affected?



# Legacy Systems Couldn't be Restored Because:

- No longer supported by vendor
- Can't function on new infrastructure



*“The destruction of servers has had the most damaging impact on the Library.*

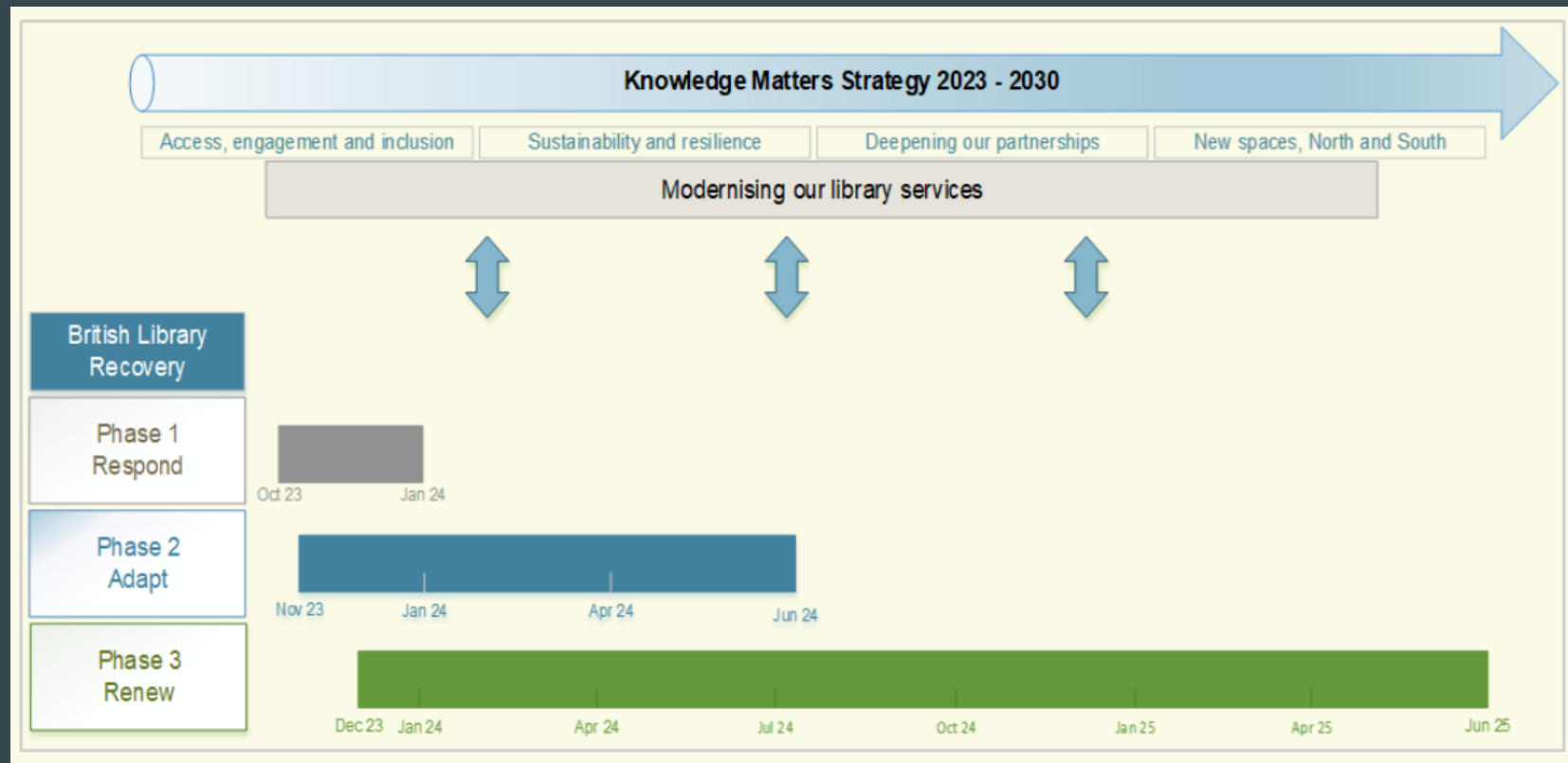
*While we have secure copies of our digital collections, we lack viable infrastructure on which to restore it.”*



# Aftermath: March 2024

- Access to only 50% physical collections; even staff access is limited
- Website down
- Digitization activity paused
- Digital collections still being brought back
- No access for researchers to journals, databases, theses...
- “Print legal deposit” received but not processed
- Failing terms of Sound Heritage grant because access is down

# Recovery Plan



# Aftermath: October 2024

## What's currently available?

We're continuing to experience disruption to our services because of a [cyber-attack](#). At the moment access to our collection and online resources is limited.

**What's available and where to find it**

# Agenda

The British Library

The Attack

The Consequences

**Lessons Learned**

# Root Cause

- **Complex network topology** failed to contain/restrict attacker activity
- Older applications rely on manual ETL processes for data transfer, increasing the volume of customer and staff data in transit on the network through **unsecured processes**
- **Legacy infrastructure** is the primary contributor to the length of time that the Library will require to recover.

# Lessons Learned

1. Enhance network monitoring
2. Retain on-call security expertise
3. Fully implement MFA
4. Enhance intrusion detection
5. Implement network segregation
6. Practice comprehensive business continuity plans
7. Maintain a holistic view of cyber risk.
8. Manage systems life cycles to eliminate legacy technology.
9. Prioritise remediation of issues arising from legacy technology
10. Prioritize recovery alongside security.
11. Increase cyber-risk awareness and expertise at the senior level.
12. Regularly train all staff in evolving risks.
13. Manage staff and user well-being in incident plans. Deeply upsetting to staff and users whose work is disrupted and compromised.
14. Review acceptable personal use of IT. Allowing personal use of network storage increases attack intrusiveness for staff members.
15. Collaborate with sector peers.
16. Implement government standards. Review and audit often.

#	Item	NIST #	NIST Name
1	Enhance network monitoring	SI-4	System Monitoring
2	Retain on-call security expertise	IR-7	Incident Response Assistance
3	Fully implement MFA	IA-2	Identification & Authorization
4	Enhance intrusion detection	SI-4	System Monitoring
5	Implement network segregation	AC-4	Information Flow Enforcement
6	Practice comprehensive business continuity plans	CP-2	Contingency Plan
12	Regularly train all staff in evolving risks	AT-2	Literacy Training & Awareness
16	Implement government standards. Review and audit often	CA-7	Continuous Monitoring



#	Item	NIST #	NIST Name
8	Manage systems life cycles to eliminate legacy technology	SA-3	System Development Lifecycle
9	Prioritise remediation of issues arising from legacy technology	SI-2	Flaw Remediation
10	Prioritize recovery alongside security	CP-10	System Recovery and Reconstitution





#	Item	NIST #	NIST Name
7	Maintain a holistic view of cyber risk	RA-3	Risk Assessment
11	Increase cyber-risk awareness and expertise at the senior level	PM-1 PM-9 RA-1	Program Management Risk Management Strategy Risk Assessment Policies



#	Item	NIST #	NIST Name
13	Manage staff and user well-being in incident plans	IR-4	Incident Handling
14	Review acceptable personal use of IT	PL-4	Rules of Behavior

# Remediation Actions

## INFRASTRUCTURE

- Rebuild legacy servers.
- Segment network
- Embrace the cloud.
- Provide robust and resilient backups.
- Enhance on-premise MFA capabilities
- Enhance privilege access management (PAM)

## MANAGEMENT

- Clear policies, procedures, and SoPs
- Standardization in development
- Compliance with mandated standards
- Stronger and more embedded governance structures

# New Risks Acknowledged

- Increased risk from new attackers from having publicly fallen victim
- Cultural change: risk that desire to return to normal business quickly will compromise plans for change
- Risk of inadequate staffing for cyber-security and cloud engineering
- Lack of understanding of complicated legacy systems may inhibit pace of recovery or lead to sub-optimal decisions. (need informed diagnosis; visionary planning; and good management objectives)
- Risks of failure to understand and account for risks in new (cloud-based) infrastructure

# \$7.5 - \$9 million

Direct Cost

*40% of the British Library's financial reserves*

# 18± months

Time to Complete Service Recovery



## Other Harms and Indirect Costs

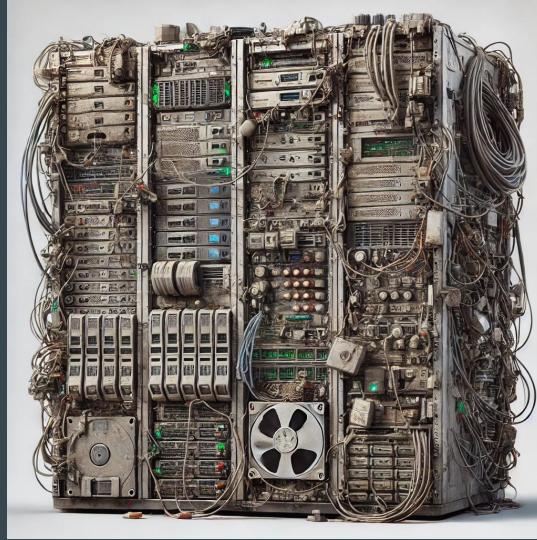
*hard to quantify*

### The Library

- Service disruptions
- Large work backlogs
- Loss of efficiency
- Grant requirements failed
- Reputational damage

### Library Customers

- Academic research blocked
- Suspended fellowships
- Business research blocked
- Delayed payments to authors
- Privacy risks



Most Consequential Finding

*“Substantial disruption of attack creates an opportunity to implement significant structural changes in ways that would otherwise have been considered too disruptive to countenance.”*

# Resources

- [Learning Lessons From the Cyber-Attack](#) (British Library)
- [British Library Annual Report and Accounts 2023/24](#)
- [#StopRansomware Guide](#) (CISA)
- [SentinelOne's explanation of Rhysida ransomware](#)

# Questions?

# License and Attribution

This material is licensed under the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Attribution: Please credit Brian Myers.

NonCommercial Use Only: Internal use permitted. Commercial use prohibited.

For full license terms, visit:

<https://creativecommons.org/licenses/by-nc/4.0>