COMMUNICATION

The 2023 Rhysida Ransomware Attack on the British Library

Prioritisation, Expertise, and Funding Issues

Frank Houghton, Michael Winterburn, and Ken Oakley

ABSTRACT

The British Library is a flagship library that plays a pivotal role in the UK learning and research infrastructure, in addition to being a central conduit for international library linkages. However, in late October 2023, this premier institution was the subject of a cyberattack that has left it crippled. The Rhysida group perpetrated this catastrophic ransomware attack. Underfunding and threat identification are explored as potential weaknesses resulting in deficiencies in the British Library's online security systems. To help prevent further such assaults in libraries, this Commentary also details what is known about the attack and how such breaches might be prevented in the future.

BACKGROUND

The British Library states that its mission is to "make our intellectual heritage accessible to everyone, for research, inspiration and enjoyment."[1] It is one of six legal deposit libraries in the British Isles, alongside the Bodleian Libraries of the University of Oxford; Cambridge University Library; the National Library of Scotland; the Library of Trinity College Dublin (University of Dublin); and the National Library of Wales. As such it is one of the premier libraries in the UK and is centrally located next to St Pancras/King's Cross railway station in central London. The British Library's collection includes approximately 170 million items and increases by several kilometres of shelf space each year. As such it is impossible to give a clear overview of its collection, which includes a high number of high prestige items.

However, the true importance of the British Library should be seen, not in high-profile items, but rather in its extensive services and activities, as well as in the breadth and reach of its collections. Table 1 provides a summary of activities conducted by the British Library, as well as a brief overview of its collections, based on two recent annual reports.[2]

Table 1 helps to demonstrate the premier and pivotal role of the British Library in the library and information infrastructure of the British Isles and further afield.

About the Authors

Frank Houghton (frank.houghton@tus.ie) (corresponding author) is Director of the Social Sciences ConneXions research institute, Technological University of the Shannon. **Michael Winterburn** (michael.winterburn@tus.ie) is Lecturer, Technological University of the Shannon. **Ken Oakley** (ken.oakley@tus.ie) is Senior Lecturer, Technological University of the Shannon.

Submitted: 18 April 2024. Accepted for Publication: 25 November 2024. Published: 17 March 2025.

https://doi.org/10.5860/ital.v44i1.17112

Table 1. Summary of activities of the British Library in recent years.

British Library 2021/22	British Library 2022/23
Custodianship	
2.25m items collected under legal deposit. Over 8,000 items received conservation treatment or intervention. 43km of linear collection items relocated in preparation for Boston Spa Renewed.	Over 2.6m items collected under legal deposit. Over 9,000 items received conservation treatment or intervention. 110,000 sound recordings made available at sounds.bl.uk.
Research	
86m collection items consulted in reading rooms, online, or remotely.	Nearly 82m collection items consulted in reading rooms, online, or remotely. Addressed nearly 86,000 reference and librarianship enquiries, to help people find what they needed. Partnered on 62 research projects alongside universities, culture and research institutions.
Culture	
237,000 people experienced Unfinished Business: The Fight for Women's Rights across the UK-wide Living Knowledge Network. Over 50,000 watched our online events from across the UK and the world; another 7,000 attended in person.	782,000 people experienced Breaking the News across the UK-wide Living Knowledge Network. Over 200,000 people engaged with our culture and learning programme in Leeds.
Learning	
Schools programme accessed by over 18,800 people online and 3,000 onsite. Over 60,000 children participated in our National Outreach Programme. 9.5m visitors to the Library's Learning website.	122,000 primary and secondary school students from across the UK participated in our Schools Programme. Over 9m visitors to the Library's Learning website. Nearly 16,000 children and young people participated in our learning programmes in Leeds.
International	
Over 700 participants from 35 countries at the National Libraries Now conference. Over 10m images now made available through the Endangered Archives Programme. Over 200 diplomatic and professional exchanges with 49 countries. 50,000 people engaged with our culture and learning programme in Leeds. Around 17,000 visits a month to the reading rooms by the end of the year. Partnered on 59 research projects alongside universities, culture and research institutions.	336 diplomatic and professional exchanges with 81 countries. Over 2m images now made available through the Qatar Digital Library, used over 2m times this year. 31 new Endangered Archives Programme projects, adding to over 12m digitised images of at-risk material

British Library 2021/22	British Library 2022/23
Business	
23,800 entrepreneurs and businesses supported across the UK. 85 locations across the UK offering business support via libraries. Over 6,600 entrepreneurs helped to weather economic challenges through the "Reset. Restart" programme.	Over 42,000 entrepreneurs and businesses supported across the UK. 101 locations across the UK offering business support via libraries. £168m of gross value added (GVA) created by businesses we've supported (since 2020).
Other highlights	
	25.3m visits to the British Library website. 517 tonnes of carbon saved through decarbonisation projects at St Pancras and Boston Spa. 11.3m items collected under digital legal deposit, since its introduction 10 years ago (not including webpages in the UK Web Archive)

Figure 1. Warning signage at the British Library (January 2024).

(Source: the authors)

Ransomware on a Global Scale

It should be noted that although the UK was the focus of this particular cyberattack, evidence suggests that the US is the leading target of countries affected by Rhysida ransomware.[3] Equally important, analysis also suggests that the majority of targets of Rhysida ransomware have been organizations providing educational services.[4] Ransomware is considered the number one threat to small and medium-sized businesses (SMBs), with one in five reporting that they have been a victim.[5] Additionally attacks are starting to use generative AI. which could lead to more advanced phishing campaigns and ransomware exploitation.[6]

The CEO of the British Library has stated:

> For better or worse, everyone working at the Library now knows a lot more about the dangers of identity fraud than we did barely six weeks ago, and I would recommend to anyone the benefit of being both forewarned and forearmed.[7]

On the basis of being both forewarned and forearmed, the following sections present a theory as to how the ransomware attack may been conducted in an effort to prevent other libraries from becoming victims in the future.

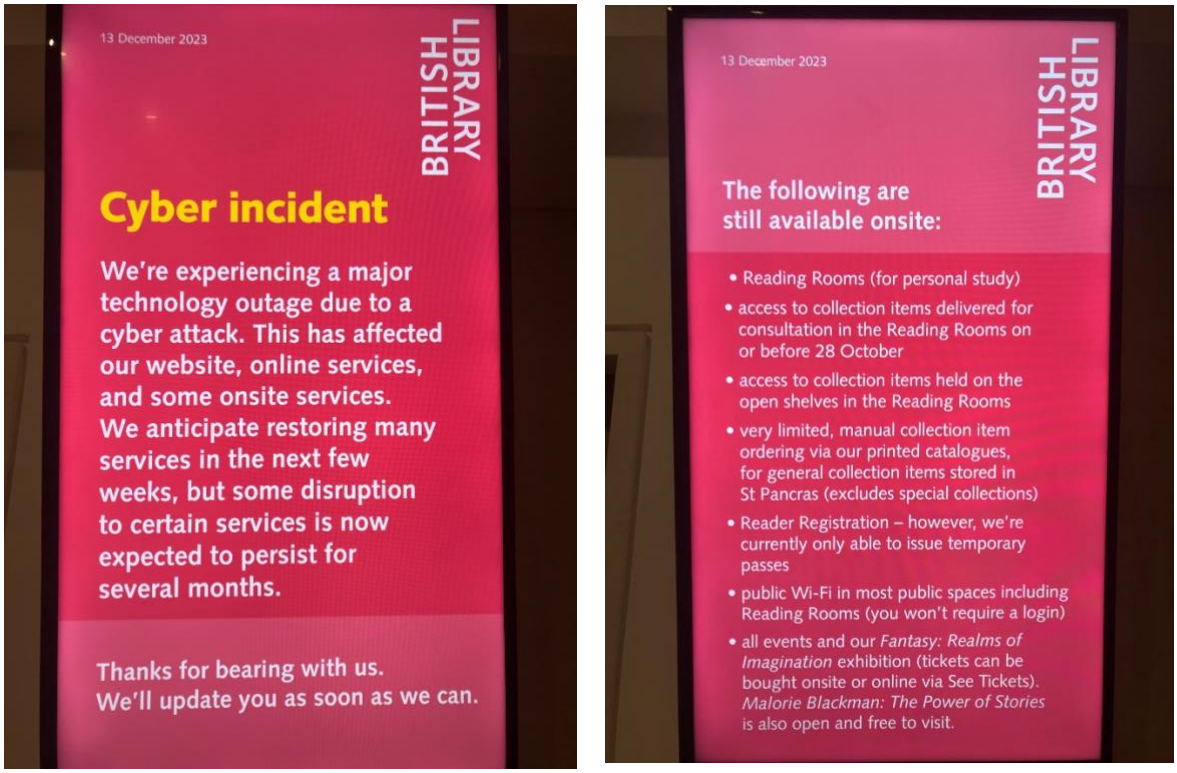
THE RHYSIDA RANSOMWARE ATTACK

In late October 2023 the British Library became aware that it had become the victim of a significant ransomware cyberattack (see figs. 1 and 2). As the CEO of the British Library has stated, "we found ourselves, that first weekend, at the receiving end of a smash-and-grab operation, and a crude attempt at extortion."[8] This attack has been described as "one of the worst cyber incidents in British history."[9]

The impact of the attack has been catastrophic with one headline reading "Cybersecurity snafu sends British Library back to the Dark Ages."[10] In the aftermath of the attack, the library website, email, Wi-Fi, cataloguing and ordering systems, as well as various interlibrary networks, were all inoperable. In addition to personnel data being penetrated, the private addresses of leading authors may have been released or sold on the dark web.[11] Six months later, the usual operations of the British Library, beyond reading room access, continued to be largely paralyzed as a result of the cyberattack. Initial hopes to restore routine operations relatively quickly have not been realized, and as of December 2024, little clear information has been released by the library (see fig. 2), while police forensic investigations continue. Most library and information professionals would probably agree wholeheartedly with the statement by Roly Keating, Chief Executive of the British Library, that "The people responsible for this cyberattack stand against everything that libraries represent: openness, empowerment, and access to knowledge."[12]

Although there is no wish to victim blame, it is important to explore some of the weaknesses that may have helped lead to the success of the Rhysida cyberattack. The most crucial element was undoubtedly inadequate in-house IT expertise due to poor funding priorities. The British Library's own report into the cyberattack noted the complexity of handling remote access from third-party providers as an obstacle to effective security.[13]

Figure 2. Warning information displayed on electronic screens at the British Library (January 2024).



(Source: the authors)

The annual reports reveal that the British Library has been engaged in numerous activities, including both expansion to its current site and the development of a new site in the North of England (Boston Spa).[14] At the same time, the library was dealing with issues such as water damage, decarbonization, and the relocation of 105km (65 miles) of linear shelved material.

Examination of the last two annual reports of the British Library reveals the minimal attention devoted to cybersecurity.[15] Close examination of these reports reveals that a cyberattack was explored as a potential threat in its risk matrices. However, in their calculations digital security rated a score of 12 alongside five other criteria that also achieved that same score.[16] This lack of a prioritization of IT services, and cybersecurity in particular, was a crucial weakness in the management of the British Library that facilitated the attack.

Despite the British Library's own report into the attack not highlighting the issue in depth, the underfunding of the public library system in the UK and of IT services generally within that sector cannot be overlooked.[17] Public libraries in the UK have endured decades of funding cuts in both real and absolute terms.[18] Funding for IT services in the UK public sector is notoriously poor, with a reliance on legacy systems being particularly problematic.[19] Goodwins has noted this underfunding, specifically about libraries:

> Unique institutions need unique security. Instead, they're fobbed off with the same old, same old…. Talk to any archivist, curator, or worker in libraries and museums, and you'll find out how little money there is, and how little of that goes on making good IT, let alone good security. Outdated and badly maintained software is a big part of why hacking groups find it cost-effective to attack badly funded public service targets.[20]

A scathing report by the Comptroller and Auditor General has also noted the UK Government's "consistent pattern of underperformance" in IT projects.[21] Public sector firms often have trouble recruiting and retaining skilled IT staff, particularly given the availability of much more lucrative contracts in the private sector. Ash gives a concrete example of this phenomenon:

> in Britain, the government's lack of investment in cybersecurity has turned the country into an open goal for potential aggressors (last year, the Treasury posted a job advert for a head of cybersecurity with a starting salary of £50,000; the median salary for a head of cybersecurity role in the private sector is almost double that number).[22]

How the Ransomware Attack Might Have Taken Place

The British Library has published a very open and transparent report on the attack, a summary of which can be seen below in table 2:

Table 2. Learning Lessons from the Cyber-Attack[23]

Learning Lessons from the Cyberattack - incident review		
Issue	**Detail**	**Further information**
Attack date	October 2023	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
Reconnaissance	Before 28 October (3 days)	Forensic analysis of the attack … 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
Source of attack	**Most likely,** the compromise of privileged user account credentials	Possibly by phishing, spear-phishing, or brute force attack
Access	First detected access at Terminal Services Server. **Exact point of entry not stated with certainty**	Not protected by multifactor authentication (MFA) due to cost but discussed and issue known Cloud services, e.g., email, Teams, and Word, had MFA
Exfiltration	600GB of files	Half a million individual documents
	Method 1: Targeted attack on Finance, Technology & People (60% of the copied files)	
	Method 2: Keywords, e.g., "passport" or "confidential" (40% of the copied files)	
	Method 3: Forcibly taking backup copies of 22 databases	

Learning Lessons from the Cyberattack - incident review		
Issue	**Detail**	**Further information**
Impact	Data and Systems encrypted	
	Servers "destructed"	"To inhibit system recovery"
	Legacy applications	Unable to be restored due to technical obsolescence, lack of vendor support, or system cannot operate in a modern secure environment
	Ransom demand	No payment made based on UK national policy (National Cyber Security Centre [NCSC])
	Cost	Process ongoing to cost new cyber secure infrastructure
	Cloud-based systems	Finance & payroll unaffected
Rebuild & Renew programme	Since December 2023	3 overlapping phases
	Phase 1: Respond	Immediate crisis management phase
	Phase 2: Adapt	6 months to identify and implement interim solutions to restore services, processes, and partnerships
	Phase 3: Renew	18 months to create a new resilient infrastructure and deliver permanent solutions by upgrades, adapting, or new solutions
Shift to Cloud-based systems	Next 18 months	
	Implement Government standards, review and audit policies and processes regularly	… 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 (Department for Digital, Culture, Media & Sports), and our new infrastructure will be built to Cyber Essentials Plus standard in recovery.

Whilst the exact details of the British Library attack are not known or have not been published, the effect was to forcibly lock all users from the network, and as the impact was so destructive, it actually may not be possible to describe definitively.[24] However, investigations by the UK National Cyber Security Centre (NCSC) and law enforcement have been conducted.[25] As the Rhysida

Ransomware group claimed responsibility for the cyberattack, including leaked British Library documents, we can reasonably postulate that they conducted the attack.[26]

Figure 3. Rhysida Group logo.[27]

Open-source reporting indicates that Rhysida ransomware actors operate as a ransomware-as-a-service (RaaS) organisation that emerged in May 2023. They use ransomware tools and network infrastructure that are leased out in a profit-sharing model. Victims have been found in multiple sectors, including education, government, healthcare, IT, and manufacturing.[28]

Gaining Access to the Network

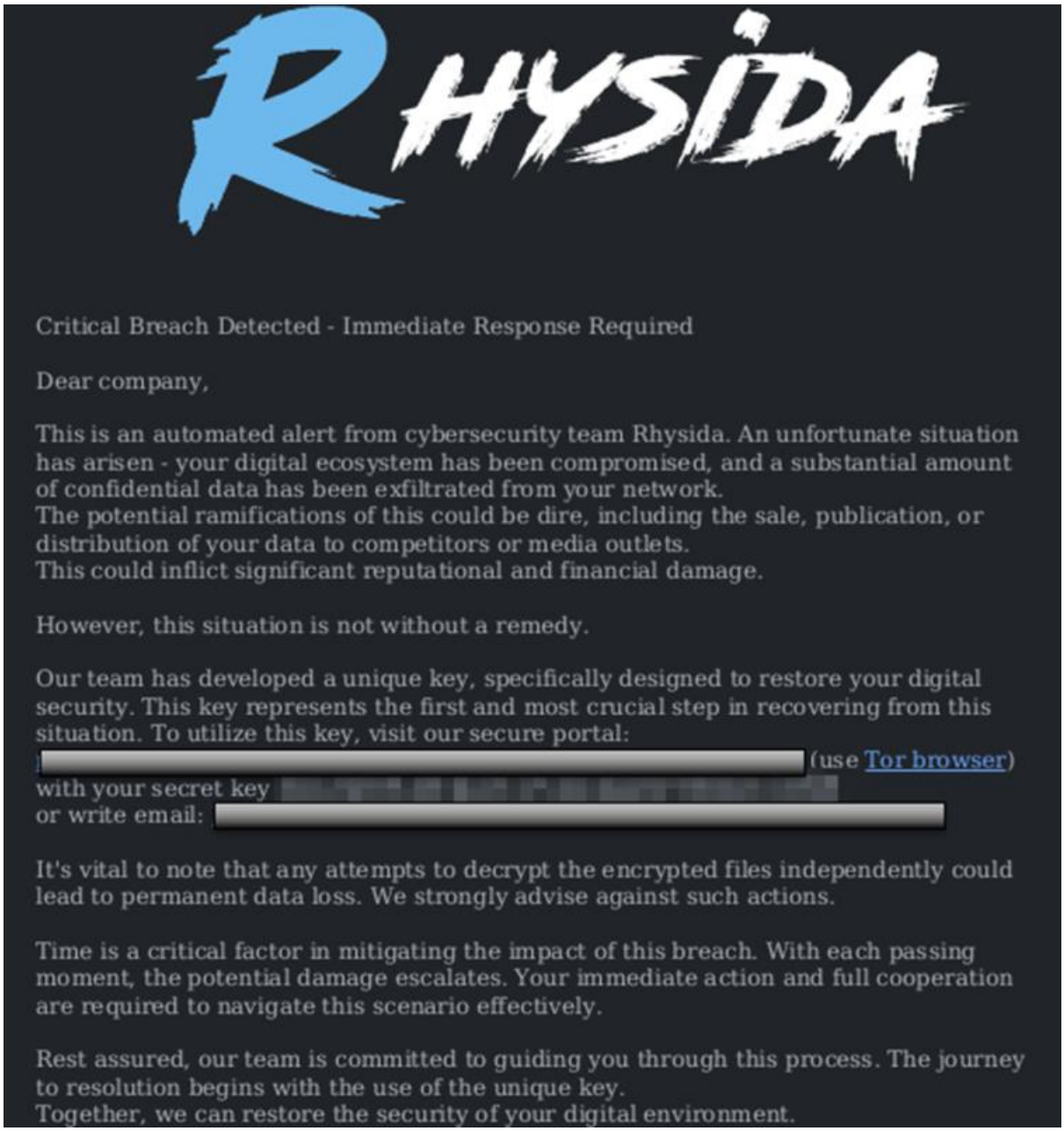
Through open-source reporting of other Rhysida ransomware attacks, we can build a theory around how the attack may have accessed the British Library computer network externally through its Terminal Services server VPN connection service and then moved through the network.[29] Since the COVID pandemic, the use of VPN connections allowing access to an enterprise network through an authenticated and encrypted communication link has become widely used. However, in the case of this attack, valid but compromised user login credentials may possibly have been discovered through a phishing attack, or simply a discovered staff member's user account with a weak password could have been used to allow the Rhysida actor to connect to the Library network remotely as that user.[30] Note that other victims of Rhysida have generally been lacking multifactor authentication (MFA) systems, which add another layer of security by requiring the user to also have access to a smartphone or computer controlled by legitimate user.[31] This MFA approach helps defend against such compromised user accounts or weak passwords.[32] Whilst the British Library was using MFA for Cloud applications, the on-premise servers, including the terminal server itself, were not protected by MFA.[33]

Living Off the Land

Once remote access to the British Library network was secured, the attack may have followed a "living off the land" attack where the Rhysida actor uses tools that are already present in the Microsoft or Linux environment, e.g., Microsoft PowerShell.[34] Such tools allow a "reconnaissance" of a network, mapping out key servers and resources. Typical commands and tools include ipconfig, whoami, nltest, net user, SSH, nmap, Remote Desktop Protocol (RDP), and so forth.[35] Rhysida normally then attack identified servers through currently known vulnerabilities. So, once a server is identified, security weaknesses in that server are exploited. For example, an unpatched server, i.e., a server that has not been updated recently, can be targeted with specific attacks. With the British Library, a vulnerable Microsoft domain controller was likely identified and then the Zerologon (CVE-2020-1472) exploit could be used to connect or login using the Netlogon Remote

Protocol (NRP).[36] Note that Microsoft patched this vulnerability in February 2021.[37] The patch prevents this Netlogon exploit if the domain controller had been updated. The Zerologon exploit allows an attacker to elevate their user permissions, i.e., to increase the ability to operate maliciously in the network as a local or domain administrator. An attacker then typically moves ”laterally,” i.e., systematically over time, in the network to discover and access other important servers and files using RDP and SSH connections and/or running PowerShell scripts.[38] Other Rhysida attacks have also used a well-known pen-testing tool called Cobalt Strike, which contains additional tools and functionality to further identify and gain access to the target's network and resources.[39] This process takes time, but if the activity has not been detected by the network management, it can take place quietly in the background until the attacker chooses to escalate to the next phase. This kind of activity using native operating systems' network commands is quite difficult but not impossible to detect by the network management system.

Figure 4. Rhysida ransom note.[40]



Encryption

Once access to a server is achieved, the Rhysida actor then typically encrypts any files of interest using the LibTomCrypt encryption tool or the ChaCha20 algorithm.[41] They would also download files from the Library network via the VPN connection to store on the Rhysida servers to sell on the dark web. Another attack possibility uses a weakness in the virtual server environment using a VMware ESXi vulnerability to access the Library's systems and then launch the Zerologon exploit, etc.[42]

Data Extortion

Rhysida uses a double extortion approach to achieve financial gain: a demand for a ransom payment to decrypt the victim's data and also a threat to publish the data if a ransom is not paid (on the dark web accessed via a Tor browser).[43] Ransoms are to be paid typically in Bitcoins, which makes it difficult for law enforcement to trace or recover. Rhysida actors normally leave a Critical Breach Detected note in PDF format (see fig. 4) with instructions for payment and possibly replacing desktop backgrounds to notify of the Ransomware attack:[44]

Rhysida demanded from the British Library a ransom of 20 bitcoin (valued at around £600,000 at the time) to restore services and return stolen data. About 600GB of material was publicly released onto the dark web as the ransom was not paid.[45]

The described steps indicate a possible approach by the Rhysida actor completing all the key stages to deliver a Ransomware attack and achieve their objective, i.e., encrypt critical files and demand a ransom. This type of assault can be seen in detail by following the attack mapped to the widely used Lockheed Martin: Cyber Kill Chain Framework, as detailed in table 3.[46]

Table 3. Lockheed Martin: Cyber Kill Chain Framework

	Lockheed Martin 7-step Cyber Kill Chain framework						
	1. Reconnaissance >	**2. Weaponisation >**	**3. Delivery >**	**4. Exploitation >**	**5. Installation >**	**6. Command & control >**	**7. Action on objectives**
Rhysida Attack							
Hacking & system tools	Initial: Port scanning, Cobalt Strike, ohishing After VPN access: cmd, ipconfig, whoami, nltest, net, secretsdump etc.	VPN access gained through compromised used account or brute force password attack	Phishing, RDP, SSH, PowerShell commands	Cobalt Strike (Beacon), Zerologon	Encryption of critical files (LibTomCrypt, ChaCha20), placing ransom note	Enabling remote access software e.g., AnyDesk > data exfiltration	Ransom demand, selling data on the dark web

Prevention Is Better Than Cure

Overall, we have presented a plausible model for the Rhysida attack on the British Library that appears to have breached the network by a combination of phishing, compromising user credentials, and exploiting vulnerabilities on servers that had not been recently patched or updated. These issues could be readily addressed through regularly educating staff regarding

phishing, implementing multifactor authentication with strong passwords, and updating all network infrastructure and servers.

The British Library has also published key lessons from the attack in its incident report paper that address technical and broader institutional issues that are helpful for similar organisations, as seen below (see table 4).

Table 4. British Library key lessons[47]

Key lessons learned from the Cyber-Attack – incident review	
Enhance network monitoring capabilities	The Library had modern tools in place, but they were not able to completely monitor or protect the network.
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.
Fully implement multifactor authentication	Multifactor authentication needs to be in place on all internet-facing endpoints, regardless of any technical difficulties in doing so.
Enhance intrusion response processes	An in-depth security review should be commissioned after even the smallest signs of network intrusion.
Implement network segmentation	No perimeter can be made entirely secure. Network segmentation is therefore essential in limiting the damage caused by a successful attack.
Practice comprehensive business continuity plans	Business continuity plans for the total outage of all systems need to be practised regularly.
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.
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 … is essential.
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.
Prioritise recovery alongside security	… the ability to quickly recover is essential when (not if) an attack is successful.
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.... The recruitment of a Board member or Board-level adviser with cyber expertise is strongly recommended.
Regularly train all staff in evolving risks Proactively manage staff and user well-being	Regular training and awareness communication … are essential for all staff, tailored to their role and level of expertise.
Proactively manage staff and user wellbeing	… include provisions for managing staff and user well-being. Cyberattacks are deeply upsetting for staff … and for users whose services are interrupted.

Key lessons learned from the Cyber-Attack – incident review	
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.
Collaborate with sector peers	Encourage collaboration and information sharing with sector peers to stay informed about common threats and best practices in cybersecurity.
Implement Government standards, review and audit policies and processes regularly	… 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.

In addition, the following gives more technical detail and is designed to help the broader community of library and information staff prevent cyberattacks in the future, based on international IT industry best practices on how to defend and recover from ransomware attacks:[48]

1. Prioritise defence against known security vulnerabilities:
    a. Update server software and operating systems
2. Enable multifactor authentication (MFA) for all external facing services, particularly for email, VPN, and accounts that access critical systems.
3. Use the principle of least privilege and provide users with only the access they need to do their job.
4. Segment or create isolated sections of the network to help prevent the spread of a ransomware attack if the network perimeter is breached:
    a. Implement subnetting
    b. Implement VLANs
5. Quickly detect and stop ransomware attacks:
    a. Use malware protection
    b. Continuously monitor directory services and network traffic
    c. Block access to untrusted web resources
6. Educate and train staff to reduce social engineering attacks, i.e., phishing via email, etc., and enforce complex passwords which require periodically changing
7. As an organisation follow a cybersecurity framework and develop a cybersecurity roadmap that includes a recovery plan that everyone in the organisation understands.[49]

Additionally, it may be important to note that the malicious encryption software used by Rhysida has been studied and a decryption tool has been successfully developed to decrypt encrypted data.[50] This tool may mitigate the effects caused by this ransomware and is freely available for download.[51]

CONCLUSION

The catastrophic ransomware attack on the British Library will undoubtedly cost tens of millions to both try and rectify, as well as to attempt to prevent future attacks. In the meantime, this pivotal institution is barely functioning at a fraction of its former capacity. Being a "community good" is no protection from such predation. Increasing numbers of libraries, universities, and museums are subject to these cybercrime attacks.[52] A crucial cause of the weaknesses in the IT systems held by these organisations is chronic and sustained under-funding, poor prioritisation of IT security, and a lack of in-house IT expertise. To preserve these institutions and facilities, this underfunding needs to be reversed as a matter of urgency. Libraries and allied organisations need to accept that they swim with sharks in a globally connected online world and that expertise in cybersecurity is now a foundational requirement. Armed with this knowledge libraries will be better prepared to take the necessary steps to safeguard their vulnerable, yet crucial, IT systems.

ENDNOTES

[1] British Library, *British Library Annual Report and Accounts 2022–23* (Department for Culture, Media and Sport and British Library, 2023).

[2] British Library, *British Library Annual Report and Accounts 2022–23;* British Library, *British Library Annual Report and Accounts 2021–22* (Department for Culture, Media and Sport and British Library, 2022).

[3] "Threat Profile: Rhysida Ransomware," SOCRadar, updated November 16, 2023, https://socradar.io/threat-profile-rhysida-ransomware/.

[4] "Threat Profile: Rhysida Ransomware."

[5] Jennifer Kurtz, "20 Cybersecurity Statistics Manufacturers Can't Ignore," National Institute of Standards and Technology, February 27, 2020, https://www.nist.gov/blogs/manufacturing-innovation-blog/20-cybersecurity-statistics-manufacturers-cant-ignore.

[6] "Ransomware Trends, Statistics and Facts Heading into 2024," TechTarget, January 3, 2024, https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts.

[7] Roly Keating, "Knowledge Under Attack. British Library," *Knowledge Matters Blog*, December 15, 2023, https://blogs.bl.uk/living-knowledge/2023/12/knowledge-under-attack.html.

[8] Keating, "Knowledge Under Attack."

[9] Lamoma Ash, "Thanks to a Shadowy Hacker Group, the British Library Is Still on Its Knees. Is There Any Way to Stop Them?," *The Guardian*, February 6, 2024, https://amp.theguardian.com/commentisfree/2024/feb/06/hacker-british-library-cybersecurity-cybercrime-uk.

[10] Connor Jones, "Cybersecurity Snafu Sends British Library Back to the Dark Ages," *The Register*, October 31, 2023, https://www.theregister.com/2023/10/31/british_library_it_outage/.

[11] Dalya Alberge and Fiona Parker, "JK Rowling's Address Could Be on Dark Web After British Library Cyber Attack," *The Telegraph*, December 5, 2023,

https://www.telegraph.co.uk/news/2023/12/05/jk-rowling-personal-data-compromised-british-library-hack/.

[12] Keating, "Knowledge Under Attack."

[13] British Library, "Learning Lessons from the Cyber-Attack: British Library Cyber Incident Review," March 8, 2024," https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf.

[14] British Library, *British Library Annual Report and Accounts 2022–23;* British Library, *British Library Annual Report and Accounts 2021–22*.

[15] British Library, *British Library Annual Report and Accounts 2022–23;* British Library, *British Library Annual Report and Accounts 2021–22*.

[16] British Library, *British Library Annual Report and Accounts 2022–23*.

[17] British Library, "Learning Lessons from the Cyber-Attack."

[18] Frank Houghton, "Caught in Crossfire: Library 'Troubles' in Northern Ireland Exacerbate Ongoing Issues," *Journal of Radical Librarianship*, 9 (2023):180–86.

[19] House of Commons Committee of Public Accounts, *Digital Transformation in Government: Addressing the Barriers to Efficiency,* Seventieth Report of Session 2022–23, September 13, 2023, https://committees.parliament.uk/publications/41388/documents/204091/default/.

[20] Rupert Goodwins, "Ransomware-hit British Library: Too Open for Business, or Not Open Enough?," *The Register,* November 27, 2023, https://www.theregister.com/2023/11/27/british_library_opinion_column/.

[21] Gareth Davies, "The Challenges in Implementing Digital Change," HC 575, National Audit Office, July 21, 2021, https://www.nao.org.uk/wp-content/uploads/2021/07/The-challenges-in-implementing-digital-change.pdf; Tim Richardson, "UK Celebrates 25 Years of Wasteful, 'Underperforming' Government IT Projects," *The Register*, July 23, 2021, https://www.theregister.com/2021/07/23/nao_govt_it_projects/.

[22] Ash, "Thanks to a Shadowy Hacker Group."

[23] British Library, "Learning Lessons from the Cyber-Attack."

[24] British Library, "Learning Lessons from the Cyber-Attack."

[25] Alex Scroxton, "British Library Cyber Attack Explained: What You Need to Know," ComputerWeekly.com, January 15, 2024, https://www.computerweekly.com/feature/British-Library-cyber-attack-explained-What-you-need-to-know.

[26] British Library, "Learning Lessons from the Cyber-Attack."

[27] "Rhysida," SentinelOne, accessed January 15, 2025, https://www.sentinelone.com/anthology/rhysida/.

[28] Rhysida Ransom Note graphic, CyberSecurity & Infrastructure Agency, accessed January 15, 2025, https://www.cisa.gov/sites/default/files/styles/medium/public/2023-11/Figure%201%20-%20Rhysida%20Ransom%20Note.png?itok=JtyDjHnc.

[29] British Library, "Learning Lessons from the Cyber-Attack."

[30] "Valid Accounts," MITRE ATT&CK, accessed January 15, 2025, https://attack.mitre.org/versions/v14/techniques/T1078/; "Phishing," MITRE ATT&CK, accessed January 15 2025, https://attack.mitre.org/versions/v14/techniques/T1566/.

[31] "Cybersecurity Framework," National Institute of Standards and Technology, accessed January 15, 2025, https://www.nist.gov/cyberframework.

[32] Rhysida Ransom Note graphic.

[33] British Library, "Learning Lessons from the Cyber-Attack."

[34] Valecia Stocchetti, "Abusing Scheduled Tasks with Living off the Land Attacks," Center for Internet Security, accessed January 15, 2025, https://www.cisecurity.org/insights/blog/abusing-scheduled-tasks-with-living-off-the-land-attacks.

[35] "Cybersecurity Framework."

[36] "Cybersecurity Framework."

[37] "Netlogon Elevation of Privilege Vulnerability," Microsoft, updated February 11, 2021, https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472.

[38] "Remote Services: Remote Desktop Protocol," MITRE ATT&CK, accessed January 15, 2025, https://attack.mitre.org/versions/v14/techniques/T1021/001/; "Remote Services: SSH," MITRE ATT&CK, accessed January 15, 2025, https://attack.mitre.org/versions/v14/techniques/T1021/004/; "Command and Scripting Interpreter: PowerShell," MITRE ATT&CK, accessed January 15, 2025, https://attack.mitre.org/versions/v14/techniques/T1059/001/.

[39] "Rhysida Ransomware," Health Sector Cybersecurity Coordination Center, August 4, 2023, https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf.

[40] Rhysida Ransom Note graphic.

[41] Rhysida Ransom Note graphic; "Cybersecurity Framework"; "Data Encrypted for Impact," MITRE ATT&CK, accessed January 15, 2025, https://attack.mitre.org/versions/v14/techniques/T1486/; Glyoon Kim et al., "A Method for Decrypting Data Infected with Rhysida Ransomware," accessed January 15, 2025, https://doi.org/10.48550/arXiv.2402.06440; LibTomCrypt (Github), accessed January 15, 2025, https://github.com/libtom/libtomcrypt.

[42] Scroxton, "British Library Cyber Attack Explained."

[43] "Cybersecurity Framework"; "Financial Theft," MITRE ATT&CK, accessed January 15, 2025, https://attack.mitre.org/versions/v14/techniques/T1657/.

[44] "Rhysida."

[45] British Library, "Learning Lessons from the Cyber-Attack"; Geraldine Kendall Adams, "Museums on Alert Following British Library Cyber Attack," Museums Association, December 20, 2023, https://www.museumsassociation.org/museums-journal/news/2023/12/museums-on-alert-following-british-library-cyber-attack/.

[46] "The Cyber Kill Chain®," Lockheed Martin, accessed January 15, 2025, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[47] British Library, "Learning Lessons from the Cyber-Attack."

[48] William C. Barker, William Fisher, Karen Scarfone, and Murugiah Souppaya, "Ransomware Risk Management: A Cybersecurity Framework Profile," NISTIR 8374, National Institute of Standards and Technology, February 2022, https://doi.org/10.6028/NIST.IR.8374; "#StopRansomware: Rhysida Ransomware," CyberSecurity & Infrastructure Security Agency, November 15, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a.

[49] "Cybersecurity Framework."

[50] Kim et al., "A Method for Decrypting Data."

[51] "Rhysida Decryption Tool," KISA, accessed January 15, 2025, https://seed.kisa.or.kr/kisa/Board/166/detailView.do.