Cyber-attack on the British Library: what happened and what we've learned

Sir Roly Keating, Chief Executive

BRITISH LIBRARY

Sharing insights to build collective resilience

- To help our peers plan and protect themselves against increasingly aggressive cyber threats we published a comprehensive cyber incident review paper
- As open about our situation as we can safely and securely describe
- Significant, sometimes uncomfortable, lessons for us – valuable for all those engaged in collecting and providing access to knowledge and culture, and delivering public services
- Increased resilience across our community of peers would be a welcome positive outcome from this deeply damaging criminal attack

Understanding the attack

- Ransomware attack on 28 October 2023 claimed by Rhysida, a criminal group rather than geopolitical
- Suspected instance of hostile reconnaissance a few days prior
- Around 600GB of data copied and exfiltrated – targeted Finance, HR, Technology Department data, and then backups of other databases
- Other data encrypted, substantial damage to applications, all users locked out, online services taken offline
- Extortion attempt, followed by auction, then publication of most of the dataset on the dark web
- Range of on-site public services continued throughout the incident

Causality

- Probable point of entry was a server set up to support remote IT access in response to Covid restrictions
- Possibly a phishing or spear-phishing attack, or a brute force attack (where passwords are repeatedly tried against a user's account)
- Legacy system not subject to Multi Factor Authentication, unlike much of the rest of the IT estate
- Cyber-security software protected parts of the network but not all. Some software was ineffective against this attack
- Attackers used disruptive and anti-forensic measures – including destruction of servers to inhibit recovery

Incident management

- Immediate shut down by IT Department to prevent further loss
- Major incident protocols immediately invoked: Gold and Silver command process
- National Cyber Security Centre called immediately
- Independent cyber experts immediately procured
- DCMS Cyber and Sponsor expertise
- Staff and stakeholder engagement
- No engagement with the perpetrators

Immediate, open engagement with sponsor team, cyber and communications teams (critical for bringing expertise to bear and enabling/controlling the flow of information)

Business continuity plans for total outage of systems need to be practiced regularly, alongside those relating to single systems

BRITISH LIBRARY

Stakeholder management

- Instinct to communicate as openly as possible, restricted by criminal investigations
- WhatsApp and staff cascade systems for key updates
- In person briefings for staff by Chief Officers
- Social media, basic interim website for external messaging
- Periodic CEO blogs to help set and clarify external narrative
- Close involvement of the Board – CEO updates and extraordinary meetings at key investigation milestones

Keep communications updated regularly, even when detail is hard to give

Seek to proactively manage the wellbeing of users and staff

BRITISH LIBRARY

Early recovery

- Safety first approach to checking the integrity of data and collection
- Service restoration – helping most of our users to access most of what they could pre-cyber through workarounds by end of Q1 24/25
- Prioritisation – for example fulfilling our statutory Public Lending Right obligations
- Some innovation, as well as drawing on institutional memory to revive pre-digital workflows
- Restoration of main catalogue in January, increasing access to Reading Room material and Special Collections, PLR statements issued and on track for payment by end of March

Technology

- Topology of our IT estate allowed significant access to attackers, modern infrastructure will be segmented and resilient
- Legacy infrastructure largely irrecoverable, slowing restoration
- Impact partially mitigated by procurement of new infrastructure that had already begun
- Permanent uplift in spend on cyber-security, accelerating already planned *Knowledge Matters* investment in digital infrastructure
- Collaboration with sector peers – common threats and adoption of best practice

Ensure MFA covers all internet-facing endpoints

Enhance network monitoring capabilities

Implement and enhance network segmentation

Prioritise the remediation of legacy tech issues and manage systems lifecycles to eliminate in future

Prioritise the ability to recover as well as security itself

BRITISH LIBRARY

Governance

- New Board committee established: Digital Portfolio Committee, with external adviser
- Oversees a new Programme – **Rebuild and Renew** (six month Adapt phase, 18 month Renew phase), along with wider Technology/Digital strategy
- Particular weight being given to change management to ensure long term culture change

Ensure holistic overview of cyber risk so that low level aggregate risks are better understood

Regular cyber risk training at all levels

Build cyber risk understanding at Board level – if possible, recruit or co-opt experts

Thank you

BRITISH LIBRARY