ROYAL NAVY MUSEUMS

Hard Lessons, Stronger Systems

Recovering a Museum after a Cyber-Attack

Presented by George Wilson, Head of IT & Amy Adams, Collections Information & Access Manager

Story of our Collections

Sites Across the UK:

- Royal Navy Museum – HMS Victory, HMS Warrior, HMS M33, Royal Marines Experience
- Naval Aviation
- Submarines
- Explosion
- Hartlepool & HMS Trincomalee
- HMS Caroline

Europe’s largest collection of historic ships.

Collection of over 3 million items.

Pre-Attack Context

Everything Digital

- Internal File Shares
- Finance
- HR
- Ticketing
- Collections Management
- Digital Asset Management
- Online Collection
- Barcoding
- Phones
- Printers

Cyber Security

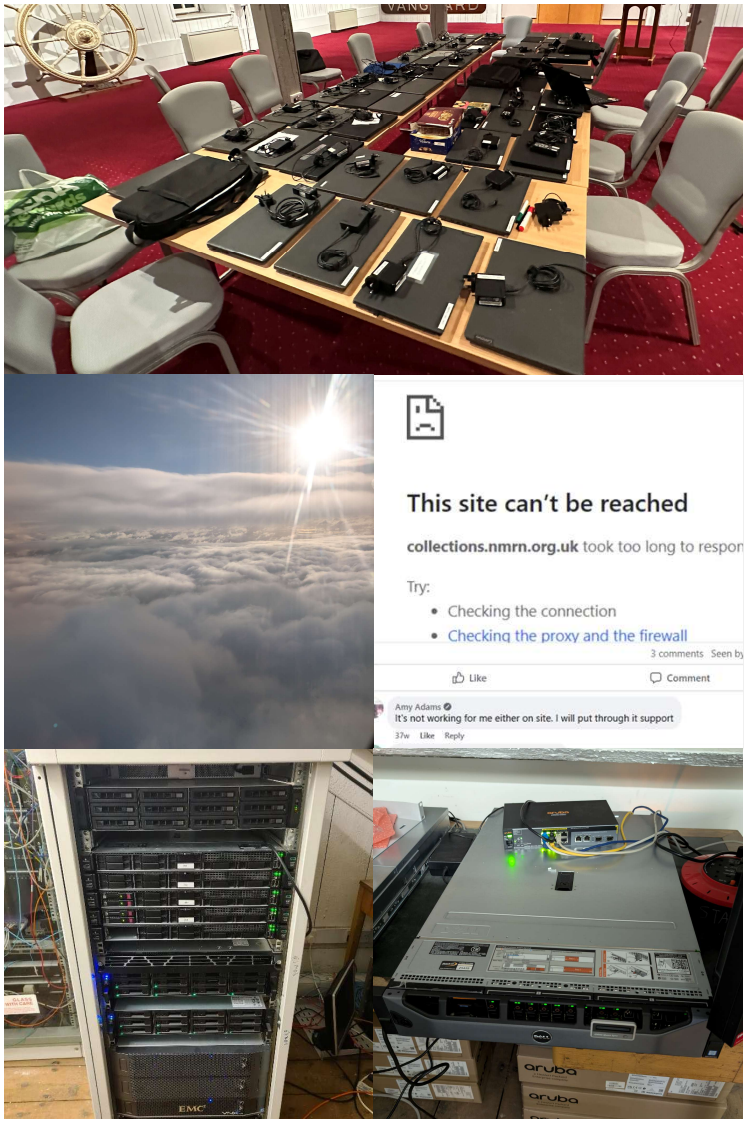
- Benchmarked British Library Lessons Learnt
- Gap Review
- Cyber Essentials Readiness Assessment
- Microsoft Conditional Access
- Penetration Testing
- Vulnerability Assessments
- Due to Implement Patch Management System

Digital Preservation Project

- TNA Resilience Funded
- Digital Preservation Plan
- Digital Preservation Working Group
- Assessment/Review of Digital Institutional Records & Archive
- Interim Digital Repository Created

Cyber-Attack - What Happened

- Attack hit at 3am on Monday 9th December 2024.
- Issues were noticed around 8am when staff arrived for the day.
- Early investigations confirmed that this was a sophisticated Ransomware attack.
- Immediate impact and damage assessment.
- Of our 20 major systems, 15 were offline.
- Communication to the wider business and stakeholders.
- To limit any further spread, an IT blackout period was implemented.



Approach to Rebuilding

Restore Core Operational Services

- Core services such as ticketing to enable museum operations
- Temporary, loaned infrastructure

Restore Staff Access

- Phased staff account access
- Device rebuilds (laptops and PCs)

Rebuild Planning

- Longer-term infrastructure planning
- Opportunity to re-design infrastructure, reviewing all options

Rebuild Implementation

- Procurement and installation of new infrastructure
- Rebuilt infrastructure from the ground up, following best practice and aligning to standards such as Cyber Essentials

Continued Service Restoration

- Alongside rebuilding, services continued to be restored, including Collections Management, printers, and phones

Implement Additional Security

- Multiple additional security measures implemented
- Solutions and systems managed in line with Cyber Essentials standards, as the minimum standard

Increasing Collections Data Resilience

Cloud vs On-premise

- Costs
- Licences
- Users
- Storage Volume
- Cyber-security

Back-Up Routines

- 3-2-1 rule
- System-tailored RPOs
- Enhanced retention

Disaster Recovery Infrastructure

- Full offsite DR
- Increased DR resources
- Decreased RTOs

Data Retention & Archiving

- Data volume
- Rot data
- Retention schedules
- SharePoint
- Digital preservation

External Data Depositing

- 3rd party partnerships
- Extra copies
- Increase access

External Access

- Secure external Collections access
- Secure 3rd party support access

Standards/Best Practice

- Cyber Essentials
- Backup and Disaster Recovery systems
- Vulnerability management
- Penetration testing
- Access control and least privilege
- Data retention
- Security Awareness Training

Other Lessons Learnt

Have copies on different infrastructure

Same impact as a fire

Rebuilding is a marathon not a sprint

Wellbeing is important

ROYAL NAVY MUSEUMS

THANK YOU

George Wilson , Head of IT – george.wilson@royalnavymuseums.org.uk
Amy Adams, Collections Information & Access Manager – amy.adams@royalnavymuseums.org.uk