



Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

THE LIBRARY OF TRINITY COLLEGE DUBLIN, THE UNIVERSITY OF DUBLIN
LEABHARLANN CHOLÁISTE NA TRÍONÓIDE, OLLSCOIL ÁTHA CLIATH

Cyber Security – Planning for Business Continuity in the Library of Trinity College Dublin

Charles Montague
(montagrc@tcd.ie)



Library services are:

- Multiple systems talking to each other
- Legacy systems mixed with new
- Analogue systems mixed with digital

Library services simultaneously:

- integrate with institutional systems (patron data etc)
- integrate with ‘internet of things’ devices
- run multiple automated data interactions between a variety of 3rd parties, (other libraries, vendors, AI services etc.)
- provide services to many thousands of users, often unregistered



Prevention and Mitigation

- Risk prevention – cyber security measures, staff training, security by design etc.
- Digital Preservation - long term storage and authentication of content

Responses against risk events take different forms

- Disaster recovery – (backups) still essential against infrastructure failure
- Business continuity - ‘ the terrible thing has happened, what do we do now’
- Digital Preservation – recovery and authentication of stored content

Planning for business continuity - an uncomfortable journey through worst cases

...Do you know what your risks are?



What are the threats to our service – what events will make us start again or do something else?

Cyber Security

Consider attack vectors:

- External and Internal

‘Bad Actors’:

- Targetted
- Commissioned (!)
- Constant opportunistic automated attack

Impact:

- Disruption
- Extortion
- Destruction of services

Infrastructure Security

IaaS - Data Centre / Server Room

SaaS

- security of vendor’s systems
- subcontracted 3rd parties

Procurement – System change

External Services – Power Grid,
Network

Physical Security

- Fire
- Theft
- Loss
- Accident



Recent major cyber security events in Ireland

HSE (Health Services Executive) – 2021

University of Galway – 2021

Munster Technological University – 2024

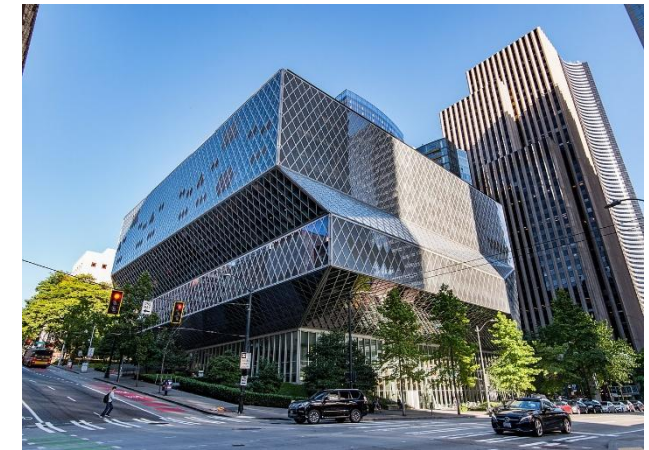
Cyber security - Major events in Libraries

British Library
October 2023



By fsse8info from UK - british library, CC BY-SA 2.0,
<https://commons.wikimedia.org/w/index.php?curid=79395961>

Seattle Public Library
May 2025



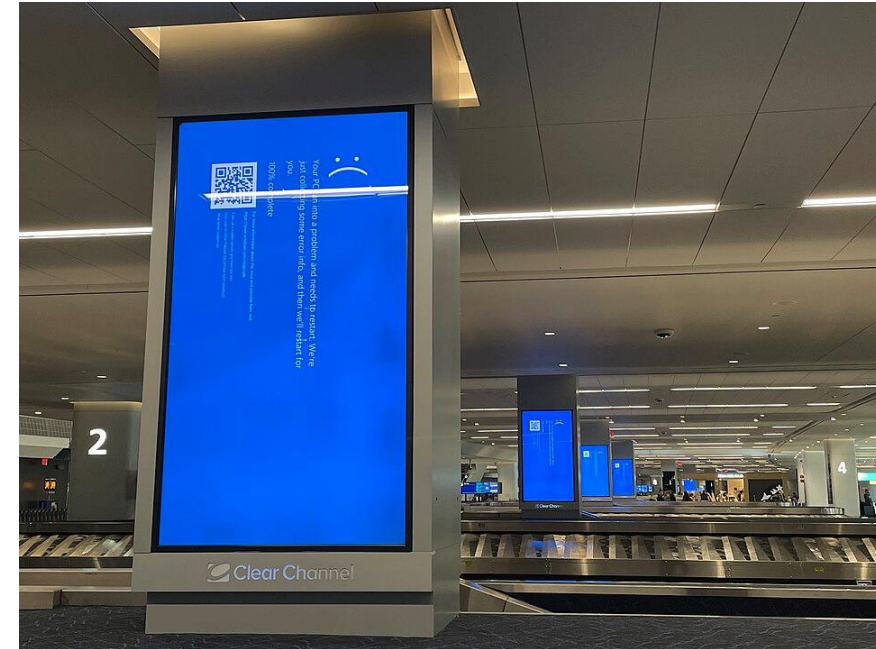
By Mj - Own work, CC BY-SA 4.0,
<https://commons.wikimedia.org/w/index.php?curid=81667872>

The second phonecall was not a cyber attack...

July 2024 - CrowdStrike Update Incident

- Estimated 8.5m affected devices
- Financial impact c.\$5.4bn (£4.1bn)
- Estimated only 10-20% of losses insured

(<https://www.bbc.com/news/articles/ce58p0048r0o>)



Blue Screens at LaGuardia airport during the CrowdStrike Incident

By Smishra1 - Own work, CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=150535443>



Recovery processes for Services and content:

Essential to have robust disaster recovery solutions in place for all digital services

- 4/3/2/1 model the current standard for data resilience
- At least one backup should be offsite, and air-gapped or fully offline.
- WORM (Write Once, Read Many)
e.g. AWS S3 Object Lock
- Checksums for content for verification

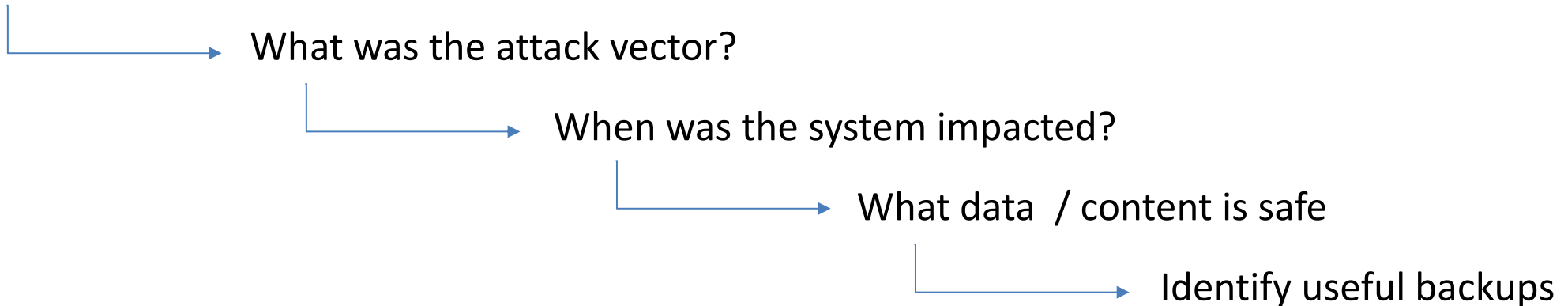
...but do you have a plan when for when there is no system to restore?



Purpose and objective:

Before an impacted system can be restored, forensic analysis needs to establish:

How was the cyber attack implemented?



Until the forensic analysis is completed, original services cannot be considered or restoration commenced.



Developing continuity plans:

Considerations:

- Plans need to be agile and responsive; situations can only be anticipated in the most general terms
- Anticipate the complexity of consolidation once original services can be restored

Highly targeted purpose:

- Short term plan for core service delivery
- Mid-term plan for extending further services
- Long-term worst case scenario



Survey of ‘stuff’ – digital; physical, intangible

- Where is it
- What is it for – content vs data
- Don’t forget the environments where services run (encryption keys, credentials etc.) and institutional memory – is it written *anywhere*?

Department [name]	Data Capture [& Frequency] Green = In Place					Other Info				Classification
Dataset	Library Business Continuity - Archive Grade capture of content	Library Sharepoint - (currently via Teams)	Library Server Backups	IT Services provide Business Continuity for service	Priority	Current Location / Version used for	Ready for Capture / Project Required	Requires Digitisation	Notes	Dataset / Content



Identify service datasets:

- Filter out content and flag for any project work required.
- What information do our services run on?
- What information is needed to start a service again from the beginning?
- What is the impact of the loss of a dataset?

Agree a Restore Point Objective (RPO) for each dataset:

- Balancing the sustainability and potential disruption of frequent capture against the nature of each service.
- How much data can acceptably be lost?



Data Output Objectives

- Output processes should guarantee malware free datasets
- Data only. No software, no content. Data should be as system agnostic as possible.
- Export data to new files
- Scan files before transfer

Storage

- Archive grade storage media
- BLU-Ray or M-discs are resilient and a useful capacity
- Consider risk assessments for selection of storage location and any additional resilience needed



Wider benefits

- High portability of datasets improved agility for service changes and system migrations
- Preservation ready knowledge management practice

Continuous process

- **Not digital preservation – GDPR and retention will apply to operational datasets**
- Build provision for continuity processes into future design
- Test outputs
- Re-run survey

THANK YOU AND QUESTIONS



Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Thank You!

Charles Montague

Deputy Head, Content Management and Open Scholarship, Digital

montagrc@tcd.ie