Dr Edmund BALNAVES

IFLA Division G Chair, IFLA

IFLA Chair, IT Section 2021-23

Director, Prosentient Systems, Australia

The library as an attack target

As custodian

Patron records, images and usage metadata
Digital resources
Physical Assets

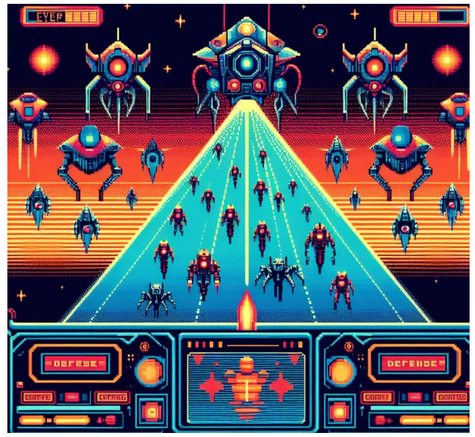
As a trusted institution

Access to information
Access to resources
Addressing the digital divide
Providing critical research resources
(e.g. Hospital libraries)

Cyber risks to the library

- Data theft (exfiltration) and blackmail
  - Patron information including financial information
  - Staff information
- Compromised services
  - Software poisoning
  - Ransomware
  - Cyber attack
  - Misuse of library network & resources
  - Passive monitoring/collection of data
- Smart buildings & Surveillance
  - Surveillance by government
    Surveillance by piggyback

Cyber defence is like playing space invaders with only one life.



British library Cyber attack

October 2023

https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf

Catastrophic impact on the library operations

Exfiltration of data

Ransomware

Unrecoverable internal systems

SDG & impact of Cyber crime

Immediate impact

- Loss of service
- Breach of patron data
- Loss of resources
- Cost of recovery
- Loss of trust
- Legal risk

Consequential impact of exfiltrated data

- Financial theft
- Impersonation
- Blackmail
- Government misuse

Compomised SDG's

Lost development opportunities

Sources of risk

External

- Exploiting weaknesses in IT infrastructure
- Unpatched / outdated software
- Exploiting weaknesses in library systems
- Software poisoning

Internal

- Click-bait risks
- Patron mis-use of library resources
- Librarian duty of care with patron data

A day in the life of cyber monitoring @ Prosentient

Web:
89,351 IP addresses actively blocked
5931 new malicious intrusion attempts (blocked)
58,431,231 hits from crawling bots
21,153,212 were AI crawling bots from Facebook,Google & others

Email:
7,491 spam emails blocked from delivery

Background monitoring
490 port scanning attempts

Defence in depth
Defensive AI bots, honeypots and log scanning (fail2ban)
Service isolation & minimum trust
Short term tokens for patron data access

It doesn’t have to go badly:

Getting on top of Security

1 **Education:**

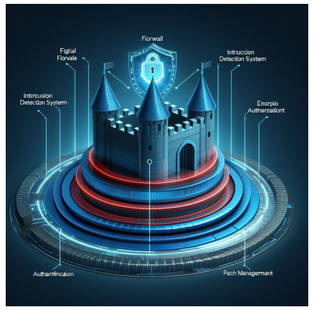
Cyber threat awareness for staff and patrons

2 **Governance:**

Invest in security Standards

3 **Defense in depth**

“trust no one”



4 **Recovery:**

Prepare for the day with DRP

Have a cyber response plan ready

Edmund Balnaves

ebalnaves@prosentient.com.au

https://www.linkedin.com/in/ebalnaves