Cybersecurity and Libraries: Global Trends, Strategy, and Best Practices

Guoying (Grace) Liu
University of Windsor
gliu@uwindsor.ca

Qing (Jason) Zou
Lakehead University
qzou@lakeheadu.ca

IFLA WLIC 2023 ROTTERDAM
World Library and Information Congress
88th IFLA General Conference and Assembly
21/25 August 2023, the Netherlands

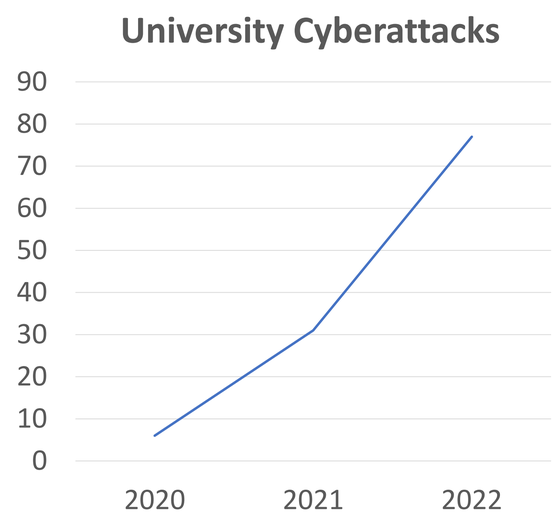
Introduction

Cybersecurity *encompasses activities, practices, and technology aimed at safeguarding computers, networks, programs, and data from unauthorized access, modification, or damage, ensuring their protection against harmful activities.*

(Kim, 2016)

Incidents

- Compromised user account
- Hacked function on a database
- Ramson attacks
- Data breaches
- More than half UK universities reported a data breach in 2020 (Irwin, 2020)
- Cybersecurity threats and threat actors become more sophisticated worldwide
- University cyberattack incidents around the world:



Country	Date	Incident
	01-07-23	Ransomware-type computer attack
	31-05-23	Software hack, data breach
	31-05-23	Data breach
	18-05-23	Cyber attack, personal data exposure
	02-04-23	University mail server hacked
	08-03-23	Ransomware
	03-02-23	Massive cyberattacks
	29-01-23	DDoS attack on website

(Source: https://konbriefing.com/en-topics/cyber-attacks-universities.html)

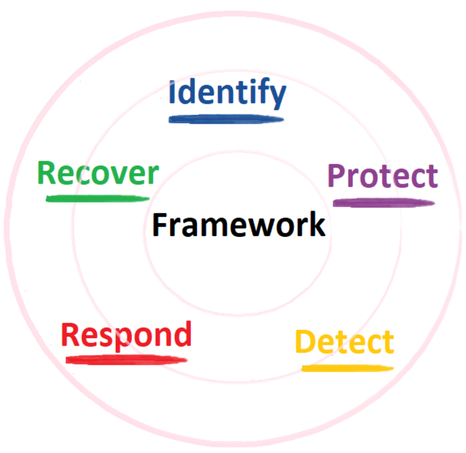
Strategy

Development

- Cybersecurity-specific strategic thinking
- Cybersecurity analysis: threats and constraints
- Develop effective plans, matching to people, process, and technology (Welch, 2019)

NIST Cybersecurity Framework

- Five core functions, comprehensive (NIST, 2018)
- Elements under each function
- Example: Identify
  - Asset management
  - Business environment
  - Governance
  - Risk assessment
  - Risk management strategy
  - Supply chain risk management



(Source: https://www.nist.gov/cyberframework)

Best Practices

Library Website

Identify

Identify cybersecurity risks pertaining to personnel, systems, applications, data, and other assets. For websites, a comprehensive analysis should encompass asset management, governance, risk management, and a range of technical details (the following list serves to demonstrate complexity but is not exhaustive):

Operating system: user management, firewall settings, TCP ports, system security patches

Web server applications: content security policies, https, server settings, web server security patches

Content management system: 3rd party integration, user management, CMS security patches

Database: user management, SQL inject attack, backup/restore

Protect

Develop and implement appropriate safegards to ensure a functioning website.

- Reduce likelihood of cybersecurity incidents from happening;
- Ensure proper access control;
- Data security (information protection produres);
- Proper regular maintenance.

Detect

Develop and implement ways to detect cyber security incidents.

- Systems to monitor logs;
- Systems to monitor access

Respond

Develop plans to react quickly and appropriately to an incident.

- Plan, analyze, communicate, and mitigate when an incident happens;
- Work with parent institutions.

Recover

Resume services without introducing additional vulnerabilities

Applicable to all library systems:

- Content management system (Drupal/Wordpress)
- EZproxy
- Omeka classic, Omeka S
- Open Journal Systems, Open Monograph Press
- Dspace, Eprints
- Cloud applications: discovery layers, hosted integrated library systems
- ……

Conclusions

- More sophisticated, more resources available compared to 2015 (Liu & Zheng, 2015)
- Keep up-to-date with security policies & IT advancements
- Follow the policies, best practices for IT & cybersecurity
- Advise, educate, train library stakeholders: awareness (institutional level strategy), security principles
- NEVER introduce new security holes when responding to cybersecurity incidents
- Collaboration with central IT, vendors, library partners

References

Irwin, L. (2020). *54% of universities reported a data breach in the past year*. https://www.itgovernance.co.uk/blog/54-of-universities-reported-a-data-breach-in-the-past-year

Kim, B. (2016). *Keeping Up With... Cybersecurity, Usability, and Privacy*, American Library Association, August 24, 2016. https://www.ala.org/acrl/publications/keeping_up_with/cybersecurity

Liu, G. & Zheng, H. (2015). Library Systems Security: On Premises & Off Premises. Canadian Library Association 2015 Annual Conference, June 5, 2015, Ottawa.

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Welch, D. (2019). Creating a Cybersecurity Strategy for Higher Education. https://er.educause.edu/articles/2019/5/creating-a-cybersecurity-strategy-for-higher-education