Cybersecurity: Best Practices for Library Systems

Guoying Liu
University of Windsor
Qing Zou
Lakehead University

Agenda

- Introduction
  - Cybersecurity Incidents, Threats
  - Cybersecurity Challenges
- Cybersecurity Strategy
  - NIST Framework for Improving Critical Infrastructure Cybersecurity
- Popular Library Systems
- Conclusions and Discussions

What Is Cybersecurity?

Cybersecurity *refers to the activities, practices, and technology that keep computers, networks, programs, and data secure and protected from harmful activities such as unauthorized access, modification, or damage*.

(Kim, 2016)

Cybersecurity Incidents

A compromised user account

A hacked function within a database

Cyberattacks on companies, governments, universities, etc.

Cyber Attack Map

54% of the UK universities in a survey reported a data breach in 2019. (Irwin, 2020)

Cybersecurity Incidents - Canada

Cyber Attacks In Canada

(Cyber Attacks In the US)

Cyber Threats - Canada

Ransomware is a persistent threat to Canadian organizations.

Critical infrastructure is increasingly at risk from cyber threat activity.

State-sponsored cyber threat activity is impacting Canadians.

Cyber threat actors are attempting to influence Canadians, degrading trust in online spaces.

Disruptive technologies bring new opportunities and new threats.

(Canadian Centre for Cyber Security, 2022)

Cybersecurity Challenges

1. Phishing
2. User education
3. Cloud security
4. High-profile information security strategy
5. Next-generation security technology planning
6. Identity and access management
7. Governance over data security
8. Unsecure personal devices

(Roscorla, 2016)

Cybersecurity Strategy

Creating cybersecurity strategy:

- Cybersecurity-specific strategic thinking
- Threats and constraints
- NIST functions matched to people, process, and technology (Welch, 2019)

NIST Cybersecurity Framework (NIST, 2018)

https://www.nist.gov/cyberframework

NIST CSF - Identify

Asset management: inventories, roles & responsibilities

Business environment

Governance

Risk assessment: asset vulnerabilities, internal/external threats, risk responses

Risk management strategy

Supply chain risk management: 3rd party partners

NIST CSF - Protect

Identity management, authentication and access control

- Identifies and credentials: issued, managed, verified, revoked and audited
- principles of **least privilege** and separation of duties
- Physical access, remote access, …

Awareness and training

Data security

- Protected, managed, maintained, verified
- Software, firmware, information, hardware integrity
- Development/testing environments separate from production environment

NIST CSF - Protect (cont.)

Information protection processes and procedures:

- Configuration change control, backups
- Policy, regulations
- Plans for response, recovery, vulnerability management

Maintenance:

Protective technology:

- audit/log records; removable media;
- The principle of least functionality

NIST CSF - Detect

Anomalies and events: Incident alert

Security continuous monitoring:

- Unauthorized personnel, connections, devices, software
- Vulnerability scans

Detection processes:

- Tested, continuously improved

NIST CSF - Respond

Response planning

Communications

Analysis

Mitigation

Improvements

NIST CSF - Recover

Recovery planning

Improvements

Communications

Library Systems - Website

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

- Operating system (Linux)
  - Security-Enhanced Linux (SELinux)
  - Kernel Patches
  - TCP ports (internal/external)
  - Firewall settings
  - User management (Physical, Remote access)
  - System logs

Library Systems - Website

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

- Web server applications (Apache/Nginx)
  - OpenSSL
  - Logs
  - Security patches
  - Strict Content Security Policy
  - Cookies

Library Systems - Website

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

- Content management system (Drupal/Wordpress)
    - Drupal security patches/regular patches
    - 3nd party integrations (e.g. google forms, calendars, chatbox)
    - Cookies
    - Google analytics
    - Logs

Library Systems - Website

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

- Database
  - Backup
  - Logs

Library Systems - E-resource Management

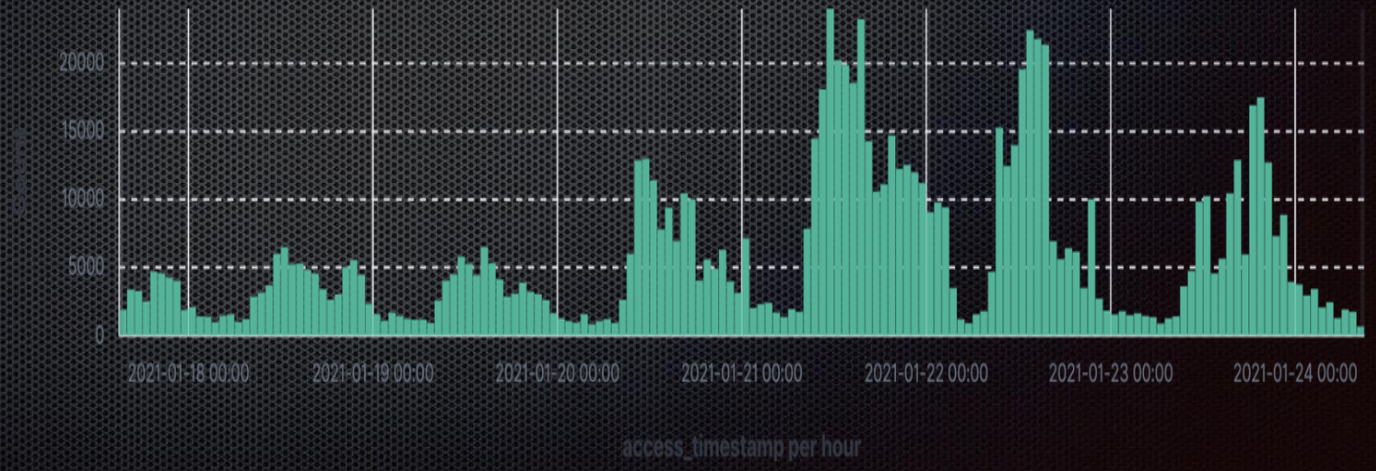
- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

- Operating system (Linux/Windows)
- Secure EZproxy
    - https (use latest, securer version: ssl, e.g. tls 1.3)
    - Check event audit records regularly
    - Authentication/Authorization: LDAP/CAS/Shibboleth
    - Stanza, log file, config file updates, …

Library Systems - E-resource Management

- Identify
- Protect
- Detect
- Respond
- Recover

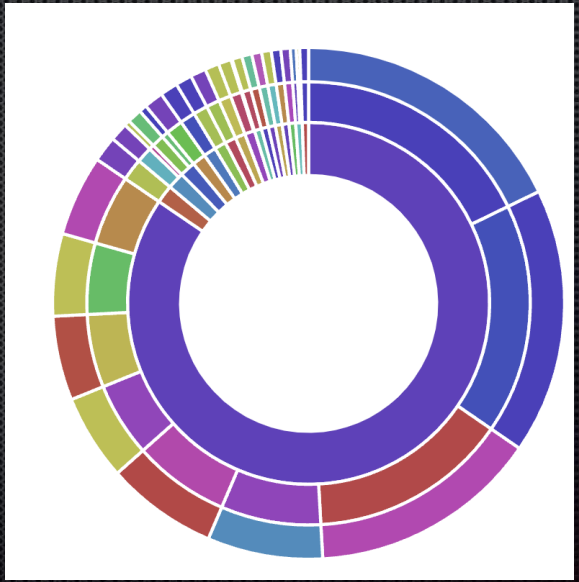
- Detect abnormal accesses



Library Systems - E-resource Management

- Identify
- Protect
- Detect
- Respond
- Recover

- Detect abnormal accesses
  - One user has multiple IPs.



Library Systems - E-resource Management

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

- Notify the user
- Block the user

ILS and Discovery Layer

- Alma/Primo: cloud – Ontario institutions
- Alma login: use institutional identity server, not internal one (ideally for backup only, not best practice); staff user (institutional/internal) pw – recommend change regularly (if cannot enforce)
- Primo login: okay
- Alma: data privacy, such as user address, phone no, student no, employee no – not included if not necessary (depends on institutional situations)

Institutional Repository

- Bepress, Dspace: local host or cloud, each situation comparison
  - Security patches: log4j (java system)
  - OS: Tomcat (Dspace)

Other systems

- Springshare
- Omeka
- OJS/OMP (Open Monograph Press)
- All systems: updates, patches, firmware - tests before implementation

Built it Right

Operate it Securely

(University of Wisconsin-Madison, 2015)

Conclusions and Discussions

More sophisticated, more resources available vs. 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

Canadian Centre for Cyber Security. (2022). *National Cyber Threat Assessment 2023–2024*. https://cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

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

Kondruss, B. (2023). *Cyber attacks news today 2022/2023*. https://konbriefing.com/en-topics/cyber-attacks.html

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

Roscorla, T. (2016). *8 Cybersecurity Challenges Facing Higher Education.* Retrieved from https://www.govtech.com/education/higher-ed/8-cybersecurity-challenges-facing-higher-education.html

University of Wisconsin-Madison. (2015). *University of Wisconsin-Madison Cybersecurity Strategy 2015–2019.* https://it.wisc.edu/wp-content/uploads/2015_UW-Madison_Cybersecurity_Strategic_Plan_Final_Jul-01-2015.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

Thank You!!

Guoying (Grace) Liu, gliu@uwindsor.ca

Qing Zou, qzou@lakeheadu.ca

Notices and Disclaimers

THIS DOCUMENT IS PROVIDED "AS-IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. YOU ARE SOLELY RESPONSIBLE FOR DETERMINING THE APPROPRIATENESS OF USING OR REDISTRIBUTING THIS DOCUMENT AND ASSUME ANY RISKS ASSOCIATED WITH IT.