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

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.

Incidents

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

<table>
<thead>
<tr>
<th>Country</th>
<th>Date</th>
<th>Incident Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>01-07-23</td>
<td>Ransomware-type computer attack</td>
</tr>
<tr>
<td>USA</td>
<td>31-05-23</td>
<td>Software hack, data breach</td>
</tr>
<tr>
<td>USA</td>
<td>31-05-23</td>
<td>Data breach</td>
</tr>
<tr>
<td>USA</td>
<td>18-05-23</td>
<td>Cyber attack, personal data exposure</td>
</tr>
<tr>
<td>USA</td>
<td>02-04-23</td>
<td>University mail server hacked</td>
</tr>
<tr>
<td>China</td>
<td>08-03-23</td>
<td>Ransomware</td>
</tr>
<tr>
<td>China</td>
<td>03-02-23</td>
<td>Massive cyberattacks</td>
</tr>
<tr>
<td>China</td>
<td>29-01-23</td>
<td>DDoS attack on website</td>
</tr>
</tbody>
</table>

(Source: https://kimbriefing.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 safeguards to ensure a functioning website.

- Reduce likelihood of cybersecurity incidents from happening
- Ensure proper access control
- Data security (information protection procedures)
- 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
- 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


