A Librarian's Guide to Cybercrime Mitigation

An ACRL Choice Webinar
October 6 2022 2pm Eastern

1. Introduction
2. Panelist Presentations
3. Interactive Exercises
4. Q&A
About SNSI

SNSI brings together publishers and institutions to solve cyber-challenges threatening the integrity of the scientific record, scholarly systems and the safety of personal data.

Members include large and small publishers, learned societies and university presses, libraries and others involved in scholarly communications.

Moderator
Gwen Evans
Member, SNSI University Relations Working Group
VP of Global Library Relations, Elsevier
Problems faced

300 Fake websites and login pages linked to 76 university library systems around the world were found in August 2018.

NCSC reports that since late February 2021, an increased number of ransomware attacks have affected education establishments in the UK, including schools, colleges and universities.

In March 2021, the City of London Police’s Intellectual Property Crime Unit (PIPCU) warned universities and students to not use ‘Sci Hub’.

The ransom a leading medical-research institution working on a cure for Covid-19 had to pay when its servers were hacked.

$1M+
Panelists

Ben Woelk
Governance, Awareness, and Training Manager, Information Security Office
Rochester Institute of Technology

Theda Schwing
Associate Director of Discovery and Delivery
OhioLINK

Carlota Sage
vCISO, Instructor
GRCIE.org
Campus and Culture

Ben Woelk
• Rochester, NY (Upstate New York, Finger Lakes Region)
• Founded 1829
• 1,524 faculty, 16,668 undergraduates, 3,050 graduate students, and 2,450 staff
• Carnegie classification R2 (Doctoral University: High Research Activity), STEM-dominant, NTID

Rochester Institute of Technology
Does your community know...

● The value of resources provided?
● Risks that impact availability of resources?
● Why access needs to be controlled?
● Who bears the costs of disruptions and why they should care?
● Why they shouldn’t provide their credentials to outsiders?
● How they are impacted by download thresholds/throttling?
How do we make good practices habitual?

Change the culture

- Contextualization
- Repetition
- Reward/Recognition
Key considerations in effecting change

- Goals
- Audiences
- Messaging
- Channels
- Partnerships
- Metrics
Partnership opportunities

- Marketing/Communications
- IT Comms/Information Security
- Third party presentations
OhioLINK

- Part of the OH-TECH consortium
- Consortium of 117 member libraries
- Wide range of institution types
- Shared print collections
- Shared e-resources
- Technology services
Workflows

● Why talk about workflows in a cybersecurity presentation?
● What’s the purpose of a workflow?
● Cross-department processes
● Make documentation available to staff
Where to Start

1. What technology services does the library use & maintain?
   a. ILS, proxy, website, vendor admin accounts, institutional repository, ...

2. Who manages each service?
   a. Vendor, IT department, library, ...

3. Does that management include:
   a. Usage monitoring?
   b. Password management?
   c. Software updates?
   d. Security patches?
   e. Backups?
   f. Digital preservation?
Handling Problems

1. Who might report a security problem?
   a. Vendors, patrons, IT, ...

2. How will a report come in?
   a. Phone, direct email, social media, ticketing system, ...

3. What is the next step after an alert comes in?
4. When is a problem resolved?
Incremental Improvements

1. Review existing documentation
2. Eliminate single points of failure
3. Build partnerships
4. Wash, rinse, repeat
Other Considerations

● **Communications from:**
  ○ IT, broader campus community

● **Communications to:**
  ○ Patrons
  ○ Staff
  ○ Vendors
Putting “U” in Security

Carlota Sage
Cybersecurity isn’t just Technology

Technology is just one pillar of cybersecurity.

Technologists and technology vendors want to believe that if we just have the right tools, we’re secure.

But tools aren’t enough.
## Where is Your Team?

<table>
<thead>
<tr>
<th></th>
<th>Grassroots</th>
<th>Team- or Compliance-Driven</th>
<th>Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organizing Principle</strong></td>
<td>Individual teams may take responsibility for security in their areas</td>
<td>Gov’t regulations or customer expectations drive security measures</td>
<td>Security is an organization-wide risk management tool.</td>
</tr>
<tr>
<td><strong>Organizational Awareness</strong></td>
<td>No common understanding of or baseline for security across org, leadership &amp; board</td>
<td>Only the teams responsible for compliance have a shared definition of security initiatives</td>
<td>Security integrated into program and product initiatives</td>
</tr>
<tr>
<td><strong>Culture</strong></td>
<td>Security seen as a “technical problem”</td>
<td>Security seen as “compliance problem”</td>
<td>Security seen as core to enabling the organization's mission</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td>Security exists as configuration of networking, laptop, software tools</td>
<td>Security tools brought in as a response to outside pressures &amp; may not be aligned with the business</td>
<td>Security tooling in place to support business alignment and risk management</td>
</tr>
<tr>
<td><strong>Ownership/Leadership</strong></td>
<td>No central cybersecurity ownership or leader</td>
<td>Security leadership exists in a silo focused on compliance</td>
<td>Security leadership enabled by and has direct access to C-Suite, Board</td>
</tr>
</tbody>
</table>
Poll: How do you come up with your passwords?

1. I have one or more passwords memorized that I rotate through
2. I have an "algorithm" in my head for creating passwords
3. I use my browser to create and save passwords
4. I use a password manager to create and save passwords
Password checker

= https://www.security.org/how-secure-is-my-password/
Poll: What do you do when you get a breach notification?

1. Ignore it
2. Delete my account and never use platform/service again
3. Change my password to the platform/service
4. Change the platform/service AND my email passwords
Breach Insight


= https://haveibeenpwned.com/
Poll: What do you do when you get an email with a suspicious link?

1. Ignore it
2. Forward it to IT/Security, then ignore it
3. Suspicious email? ALL email is suspicious!
URL Checker

= https://www.virustotal.com/gui/home/url
Q&A

if you have suggestions for other topics for future cybersecurity webinars, please put them in the chat

Thank You!
https://snsi.info/