Scholarly Networks Security Initiative

May 9, 2024

Gwen Evans

VP of Global Library Relations , Elsevier

Member, University Relations Working Group, Scholarly Networks Security Initiative

About the Scholarly Networks Security Initiative

- The Scholarly Networks Security Initiative (**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.

LIBRARY

ACADEMIC
IT SECURITY

RESEARCH

PUBLISHING

SNSI Scholarly Networks Security Initiative

Did you know?

300

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

3rd largest

The UK's National Cyber Security Centre lists the education sector as the 3rd largest target for cybercrime, ahead of retail.

Over 400

Universities and institutions across 41 countries have had their networks and data comprised by illegal website SciHub.

$1.14M

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

Catalysts for Our Conversation

sky news

Sci-Hub: Police warn students and universities against using 'the Pirate Bay of science'

Sci-Hub has been described as "the Pirate Bay of science", but often receives praise for opening access to research.

THE CHRONICLE OF HIGHER EDUCATION

Cyberattacks Are Spiking. Colleges Are Fighting Back.

The Washington Post
Democracy Dies in Darkness

Justice Department investigates Sci-Hub founder on suspicion of working for Russian intelligence

CHEMISTRY WORLD

Why do higher educational institutions keep getting hacked?

BY DALMEET SINGH CHAWLA | 8 APRIL 2021

UK's cyber security centre warns of increasing attacks on university computer networks

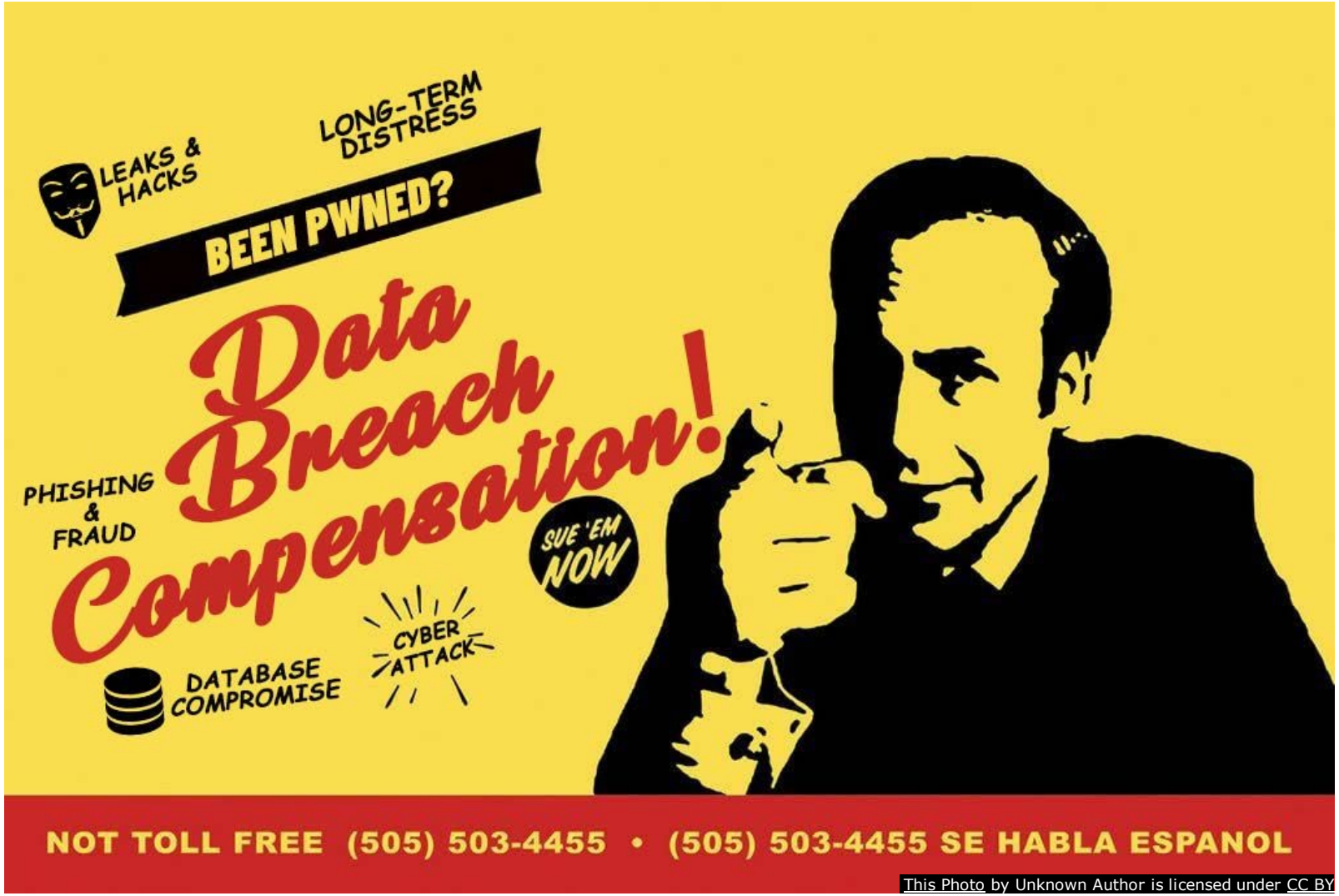
Two Resources

Nguyen CD, “Digital cultural heritage in the crossfire of conflict: cyber threats and cybersecurity perspectives,” Insights, 2024, 37: 7, 1–11; DOI: https://doi.org/10.1629/uksg.647

British Library. (2024, March 8). Learning lessons from the cyber-attack: British Library cyber incident review. https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf

What makes a soft target?

What's the Legal Risk?



This Photo by Unknown Author is licensed under CC BY

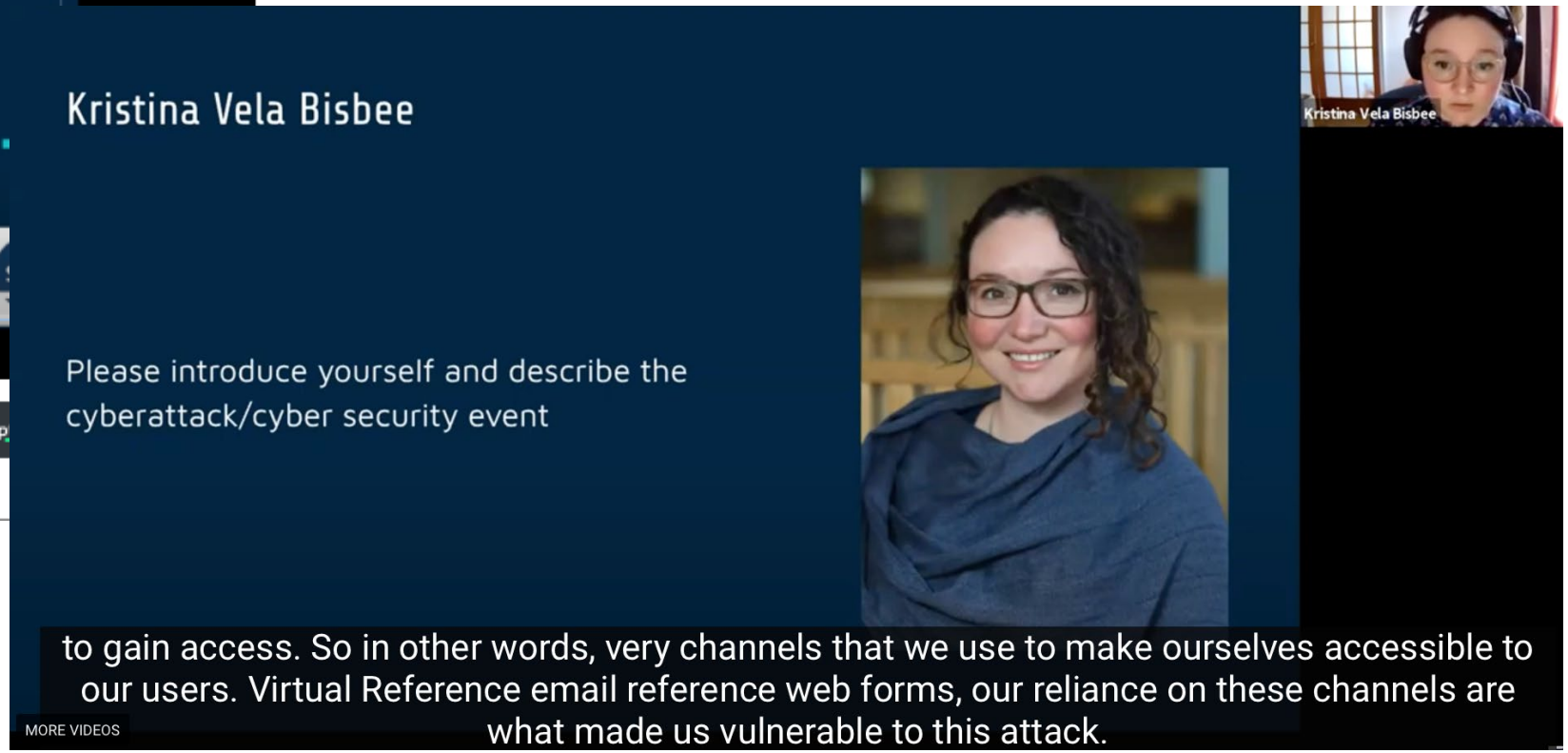
Physical/Digital Environment and Objects

Circulation Desk, Benjamin Franklin **Library**, Mexico, from National Archives https://catalog.archives.gov/id/23932427

Gone Phishing: Service Continuity after a Cyber Attack

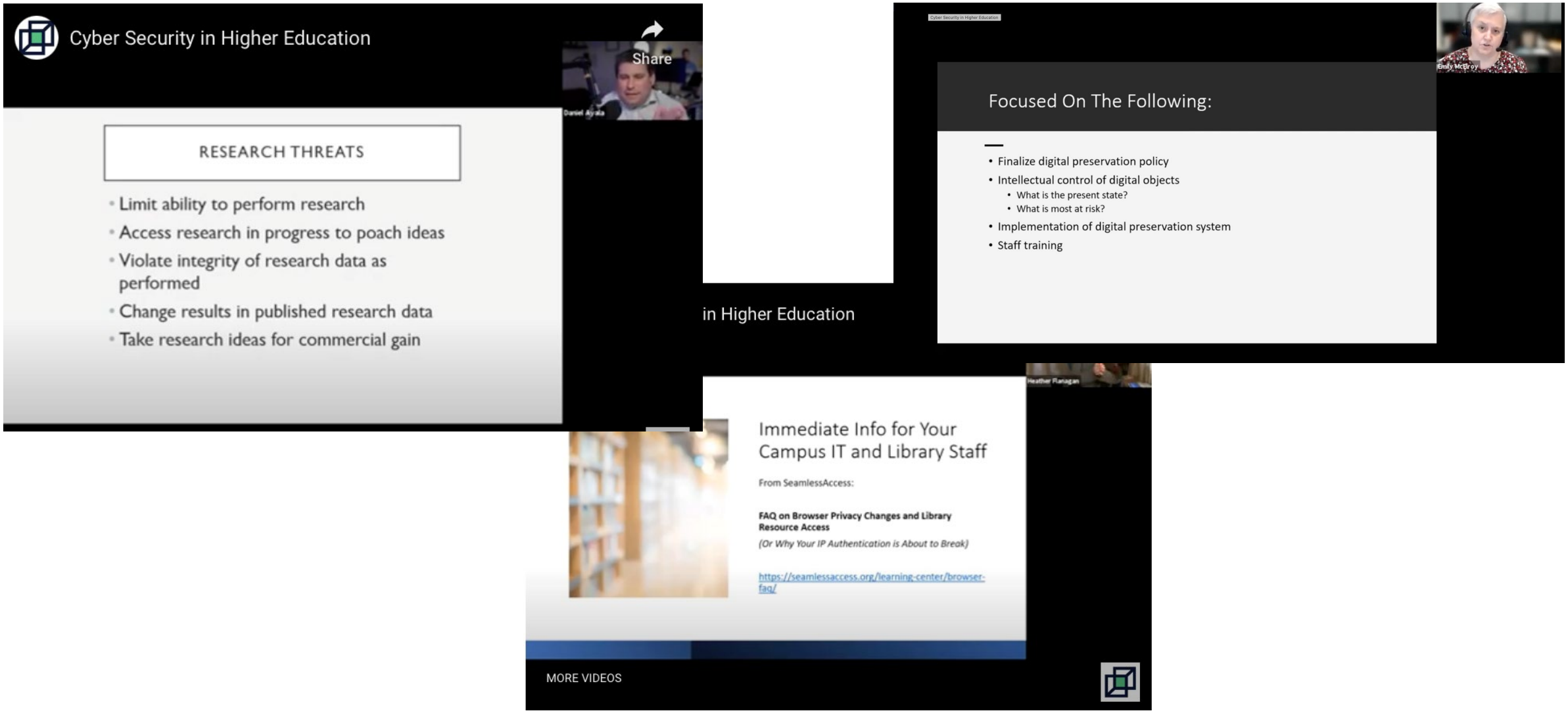
ACRL Choice SNSI Webinar https://www.choice360.org/webinars/gone-phishing-service-continuity-

Is your library prepared for a cyber attack?



Cyber Security in Higher Education

ACRL Choice SNSI Webinar https://www.choice360.org/webinars/cyber-security-in-higher-education/



A Librarian's Guide to Cybercrime Mitigation

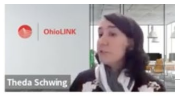
ACRL Choice SNSI Webinar https://www.choice360.org/webinars/a-librarians-guide-to-cybercrime-mitigation/

How can librarians mitigate risk and proactively protect against cybersecurity threats?

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?

Where is Your Team?



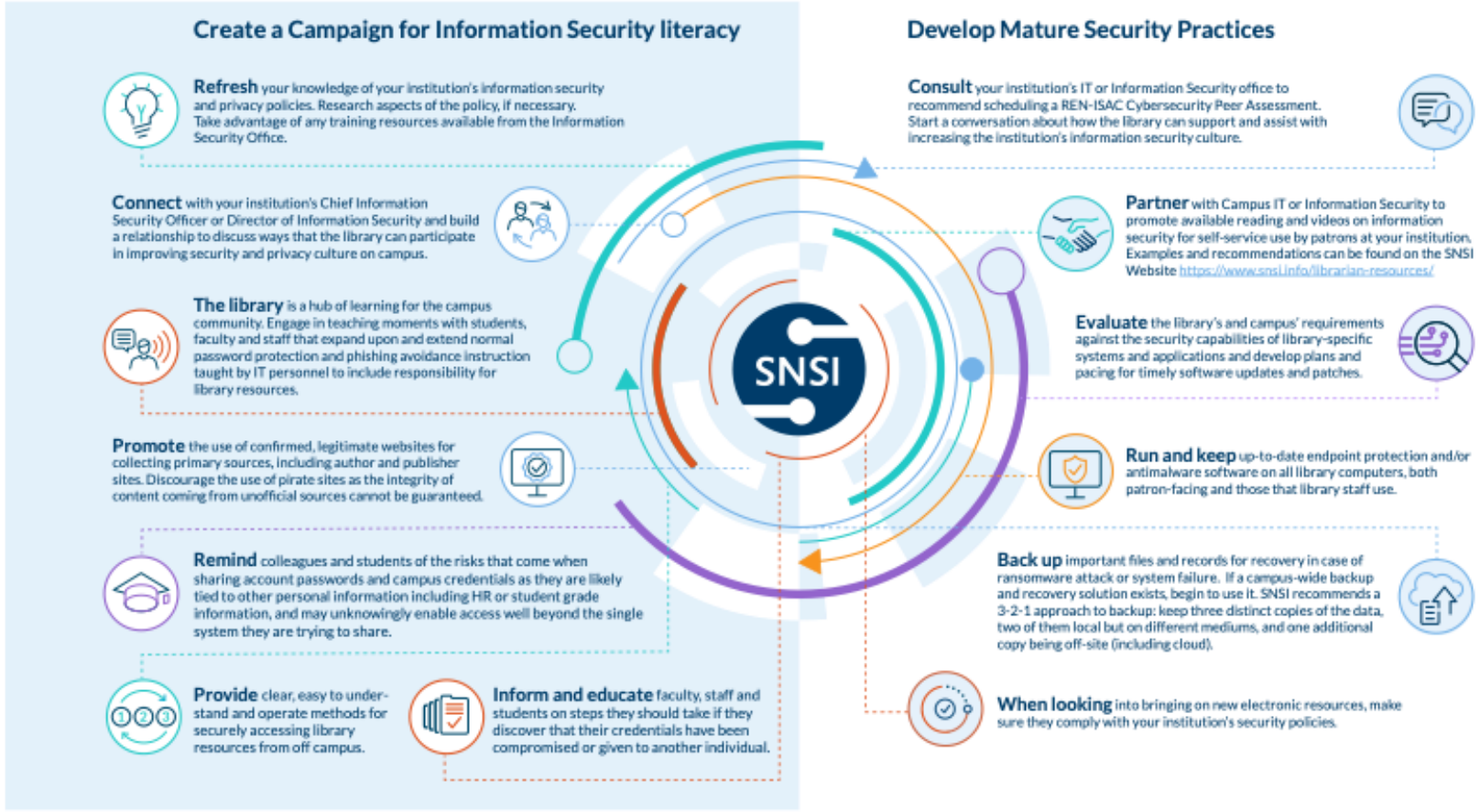
	Grassroots	Team- or Compliance-Driven	Risk Management
Organizing Principle	Individual teams may take responsibility for security in their areas	Gov't regulations or customer expectations drive security measures	Security is an organization-wide risk management tool.
Organizational Awareness	No common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

SNSI

SNSI tips for academic librarians on building strong information security defenses at your institution

The Scholarly Networks Security Initiative recommends these rules of thumb when considering how libraries can contribute and support information security practices in higher education. These same recommendations can also be applied to nearly any other organization too. The investment of time, focus, and technology in prevention efforts is far more useful than the significant costs that result after a security intrusion or data breach.

Security is the responsibility of everyone within an organization, to protect institutional data, that of faculty, staff and students, and to ensure the integrity of the work and research the institution performs. However, this investment in protecting information must be visibly supported from leaders across the organization to establish and reinforce a strong security culture on campus.



Librarians and libraries have long been champions of good security to uphold the values core to the library. The campus-wide efforts to protect data are increasing as threats against institutions' data rise. Libraries, in partnership with other administrative units across campus including IT and Information Security, can educate patrons on how to protect institutional and personal information, access genuine resources to support their research, and build strong relationships between the Library and campus Information Security colleagues.

Scholarly Networks Security Initiative (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. www.snsi.info

https://www.snsi.info/media/dlmgarxk/snsi_security_a4_page_220722.pdf