

#snsisecurity2020

The purpose of this virtual security summit by The Scholarly Networks Security Initiative (SNSI) is to discuss security threats to the research ecosystem with the aim to engender closer collaboration between publishers and academics in dealing with threats.

Time Start	Time End	Topic/Session	Speaker/Moderator
11:00 AM	11:15 AM	Opening Remarks	Nick Fowler, Chief Academic Officer, Elsevier
11:15 AM	11:45 AM	KEYNOTE: A university Chief Information Security Officer's (CISO) purview of security threats & opportunities for collaboration in combating them	Corey Roach, CISO, University of Utah
11:45 AM	12:15 PM	The threat presented by Sci-Hub and other state-sponsored or individual bad actors	Crane Hassold, Sr. Dir of Threat Research, Agari
12:15 PM	12:45 PM	LUNCH	
12:45 PM	1:15 PM	Library patron security and why it's important	Linda Van Keuren, Assistant Dean for Resources & Access Management, Georgetown University Medical Center
1:15 PM	1:45 PM	Foreign interference in academia	Joe DeMarco, Partner, DeVore & DeMarco LLP
1:45 PM	2:00 PM	BREAK	
2:00 PM	2:30 PM	How federated authentication helps with security	Tim Lloyd, CEO, LibLynx
2:30 PM	3:15 PM	Roundtable discussion with speakers	Rick Anderson, University Librarian, Brigham Young University Steven Inchcombe, Chief Publishing & Solutions Officer, Springer Nature
3:15 PM	3:30 PM	Closing remarks	

#snsisecurity2020

 THE UNIVERSITY OF UTAH®

Security Collaboration for Library Resource Access

Corey Roach, CISO
University of Utah

SNSI Security Summit
October 2020

Corey Roach

- Chief Information Security Officer (CISO)
- Joined the University of Utah in 1998
- 18+ years of Information Security Experience in Higher Ed
- Information Security Office - 34 Employees
 - Enterprise Security (Engineering, Incident Response)
 - Security Assurance (Security Operations Center)
 - Governance, Risk, and Compliance
 - Identity and Access Management

An Interesting Challenge

Unique Privacy Requirements

Fragile Assets

Limited Resources

Limited Legal Support



Threat Vector

Phishing

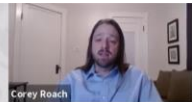
Social Engineering

Credential Re-Use

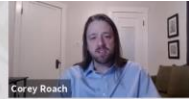
Hacktivism



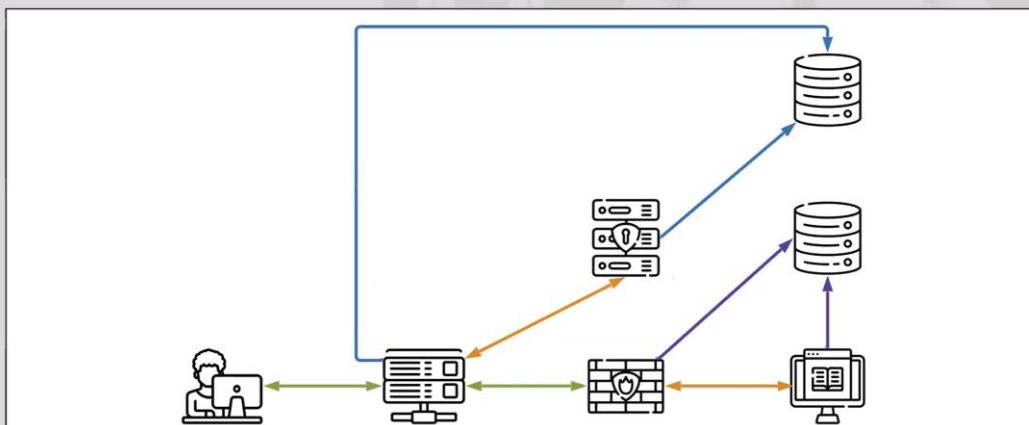
Technology alone does not
solve “*People Problems*”



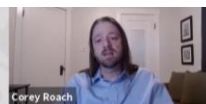
Technology Overview



Typical Library Proxy Service



Typical Logs



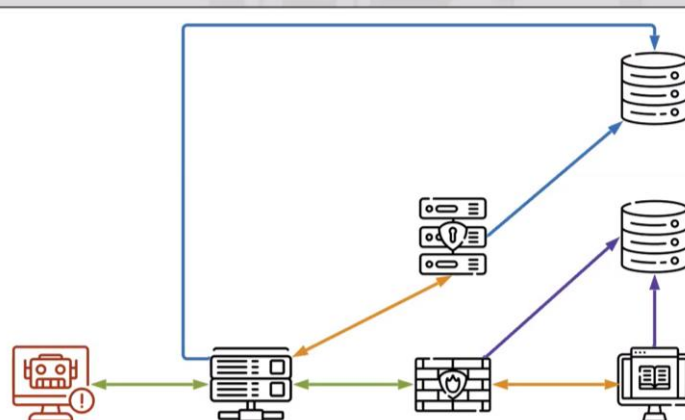
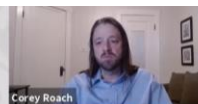
Library Logs:

- Timestamps
- Basic Browser Info (UA)
- Username
- Customer IP
- URLs Requested

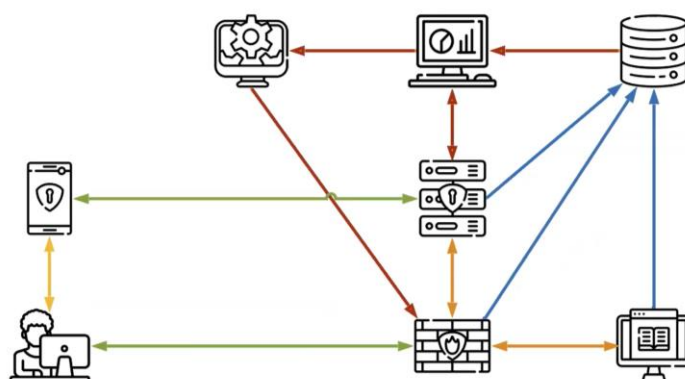
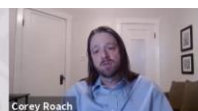
Publisher Logs

- Timestamps
- Proxy IP
- URLs Request

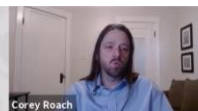
Typical Library Proxy Service



Typical Web App



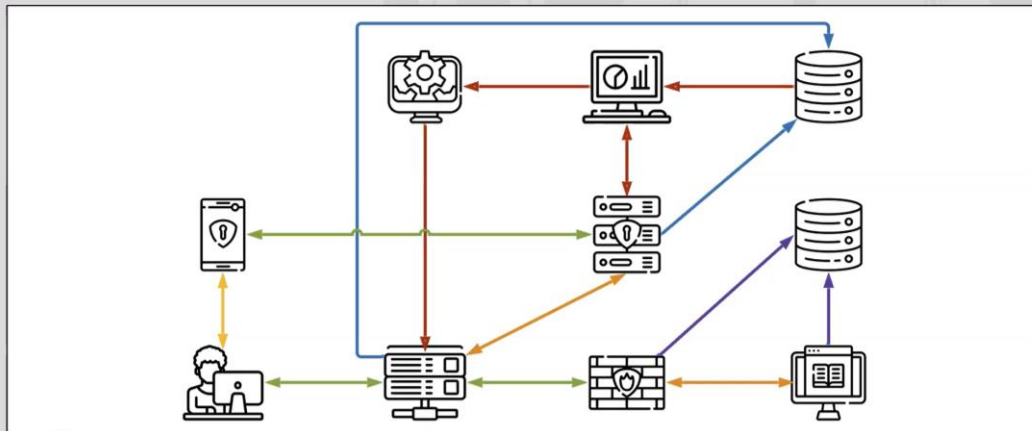
Typical Web App - Logs



Web App Owner Logs:

- Timestamps
- Extensive Browser Info
- Username
- Account Information
- Customer IP
- URLs Requested
- 2-Factor Device Info
- Geographic Location
- User Behavior
- Biometric Data
- Threat Correlation / Info Sharing

Modern Library Design



Modern Library Design



Library Logs/Info:

- Timestamps
- Extensive Browser Info
- Username
- Account Information
- Customer IP
- URLs Requested
- 2-Factor Device Info
- Geographic Location

• User Behavior

- Biometric Data
- Threat Correlation / Info Sharing

Publisher Logs:

- Timestamps
- Proxy IP
- URLs Request

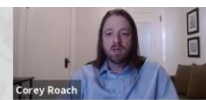
Obstacles?

Privacy
Expertise
Cost



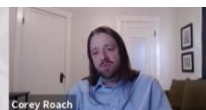
Publisher / SNSI Support

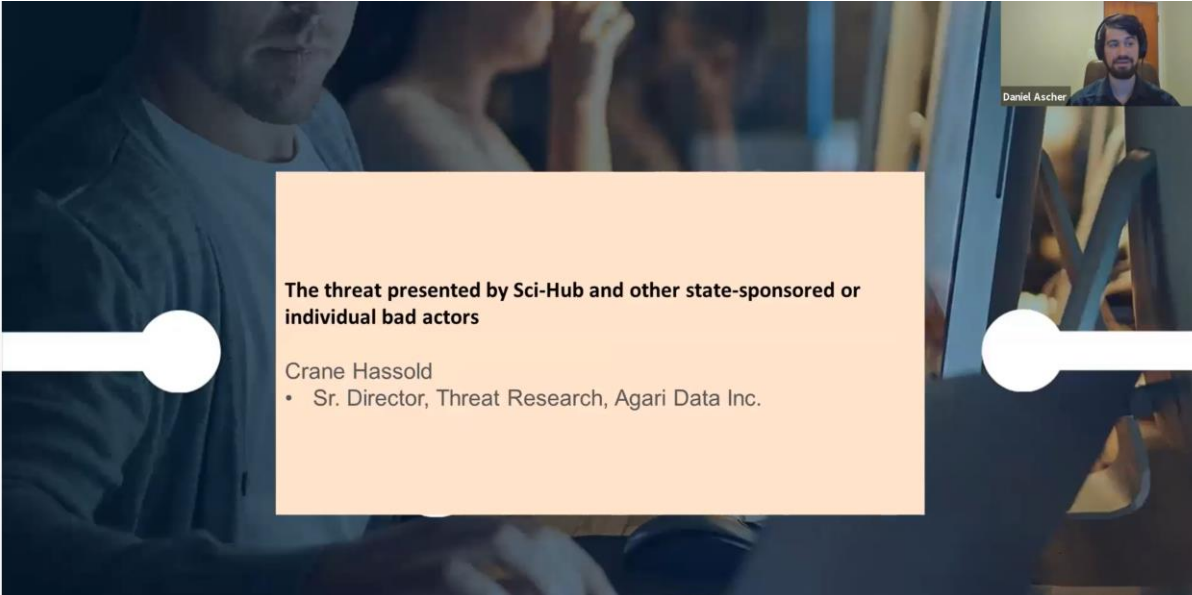
- Develop or subsidize a low-cost proxy or plug-in
- Facilitate threat information sharing
- Provide administrator training
- Promote community
- Provide pricing incentives to share risks



Other Opportunities

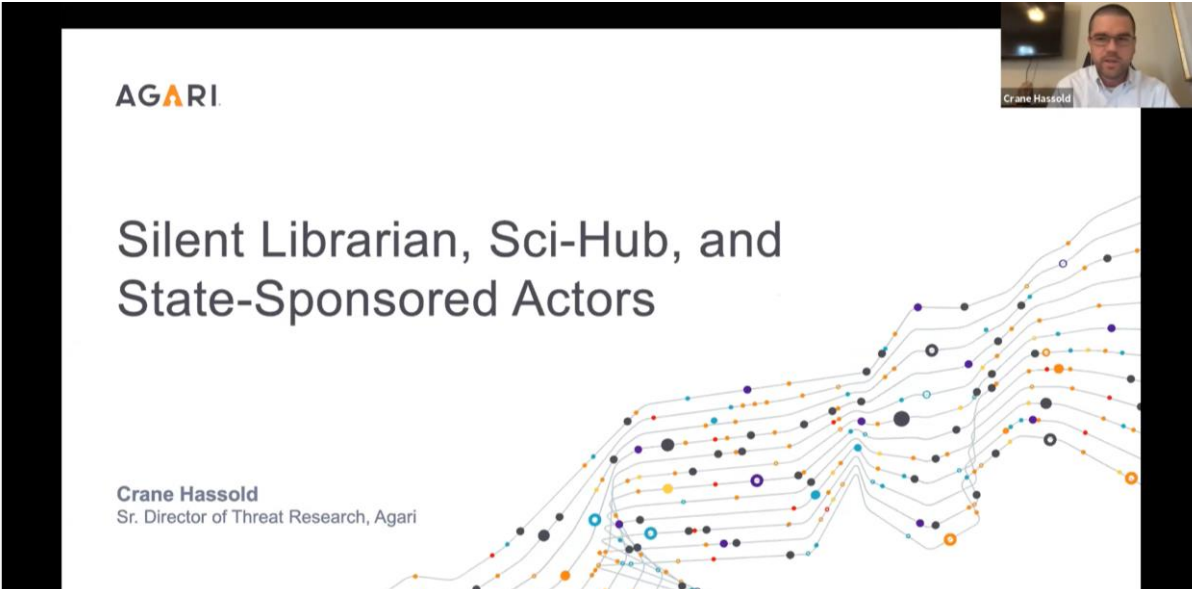

- Foster security advocates, provide materials
- Educate leadership on shared risks
- Educate users on personal risks
- Promote to customers the value of publishers





The threat presented by Sci-Hub and other state-sponsored or individual bad actors



Crane Hassold
• Sr. Director, Threat Research, Agari Data Inc.




AGARI

Silent Librarian, Sci-Hub, and State-Sponsored Actors


Crane Hassold
Sr. Director of Threat Research, Agari



Who Am I?



- 11 years in the FBI
- Helped create the FBI's Cyber Behavioral Analysis Center (CBAC)
- Built two phishing threat intelligence teams
- Currently oversee the Agari Cyber Intelligence Division
- Focus is Business Email Compromise (BEC)



Silent Librarian: An Overview



- Active since 2013
- Linked to Iranian threat actors
- Targets global colleges/universities
 - 300+ schools in 22 countries
- Phishing pages mimic library login pages
- Purpose is to compromise student/faculty credentials
- Motivation?
 - Theft of academic journal articles
 - Theft of other sensitive research?

The screenshot shows the login page for Durham University Library and Heritage Collections. It features the university's crest and logo. The page has a 'Login to Library and Heritage Collections' heading. Below this are input fields for 'Username' and 'Password'. There is a 'Don't Remember Login' checkbox and a 'Login' button. A link for 'Forgot your password?' is also present. On the right, a note states: 'Research and study materials provided through Durham University Library'. At the bottom right, a message says: 'If you are having problems using Library e-resources, email our e-resources team.'

AGARI

Silent Librarian: Attack Process



- Lure emails from university "library"
 - Consistent for years
 - Direct spoofing of university addresses
 - Use of shortened URLs behind look-alike URLs
- Phishing URLs very similar to legitimate URLs

Dear Student,

This is an automatically generated email from IT Services, Carleton University. IT Standard for Computer Passwords and System Access Controls state that an appropriate library access renewal process is implemented at Carleton University. Our records indicate that your library enrollment [REDACTED] is set to expire on January 30, 2020 12:00. For security reasons, please click the URL link below to update your library enrollment:

[University Library](#)

If you have not renewed your library enrollment by the date mentioned above, your access to the library and its associated services will expire. If you have any questions arising from this message, please contact the Library Helpdesk. For a list of the current library online services, please visit:

<https://library.carleton.ca>

Yours sincerely,

MacOdrum Library - Carleton University
1125 Colonel By Dr, Ottawa, ON K1S 5B6, Canada
library.services@carleton.ca

Legitimate URLs

shibboleth.mcgill.ca
libproxy.library.unt.edu
librarysso.vu.edu.au

Phishing URLs

shibboleth.mcgill.ca.iftl.tk...
libproxy.library.unt.edu.itlib.me...
librarysso.vu.cvrr.me...

AGARI

Silent Librarian: Links to Mabna Institute

- March 23, 2018: USDOJ indicts 9 Iranian individuals connected to the Mabna Institute
 - \$3.4 billion in intellectual property loss
 - 31.5 TB of academic data stolen
 - ~8000 university account compromised
 - Also targeted government agencies, private companies, and international NGOs
- Silent Librarian = Mabna Institute



AGARI

Silent Librarian: Indictment Aftermath

- Worked with REN-ISAC to mitigate phishing sites
- April 11, 2018: Testified at House committee on foreign threats to US research and academic institutions
 - Other witnesses focused on *physical* threats
- Indictments have had no impact on deterring future attacks



AGARI

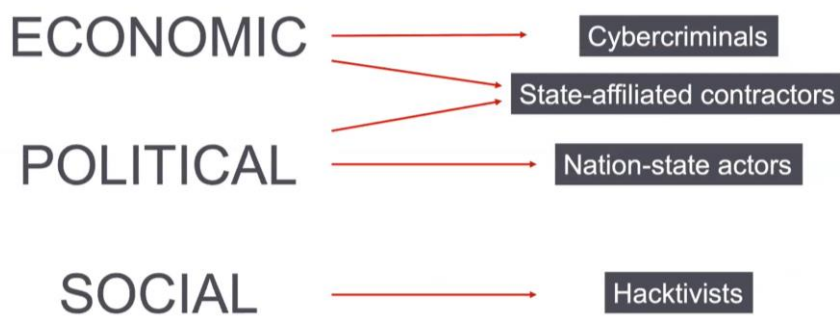
Sci-Hub

- Launched in 2011 by student in Kazakhstan
- Contains pirated copies of academic journal articles
 - 81 million+ articles
- Top countries using Sci-Hub: India, China, US, Brazil, Iran
- How do they get articles?
 - "Donated"
 - Phishing?
 - Potential link to Silent Librarian?



AGARI

Motivations for Cyber Attacks



AGARI

What Motivates Silent Librarian and Sci-Hub?



ECONOMIC

Silent Librarian

- Access to journals sold on Iranian marketplaces

Sci-Hub

- Created in response to high cost of journal paywalls
- “Napster for journal articles”

AGARI

What Motivates Silent Librarian and Sci-Hub?



POLITICAL

Silent Librarian

- “Acted at the behest of the Iranian government”
- Potential for intelligence gathering

Sci-Hub

- Potential backing by Russian government?

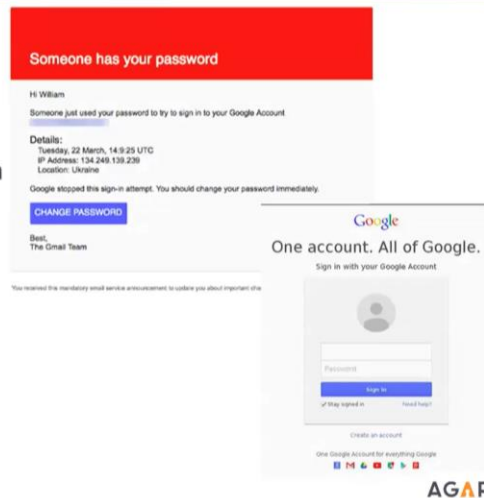
AGARI

Nation-State Actors: Myths vs. Reality

- Biggest difference between cybercriminals and nation-state actors:
 - Cybercriminals driven by **profit**
 - Nation-state actors driven by **mission**
- Not all nation-state attacks are *technically* sophisticated
 - DNC Compromise – basic Google Accounts phishing page

vs.

- Recent GRU indictments – NotPetya, Olympic Destroyer, BlackEnergy, etc.



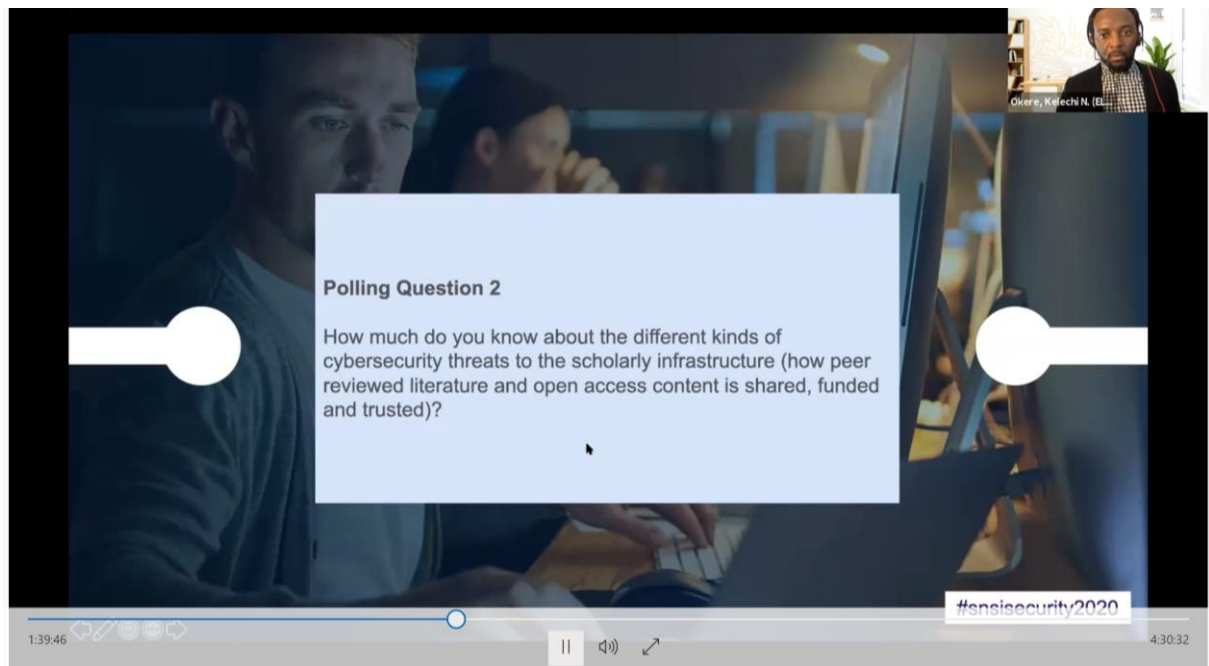
Thank You

Crane Hassold | Sr. Director of Threat Research
chassold@agari.com
@CraneHassold

Agari Cyber Intelligence Division (ACID)
<https://acid.agari.com>

AGARI





A video player interface with a background image of two people working at a computer. A light blue box in the center contains a poll question. In the top right corner, there is a small video feed of a man. The bottom of the player shows a progress bar, a play button, and a volume icon. The hashtag #ensisecurity2020 is visible in the bottom right corner of the video frame.

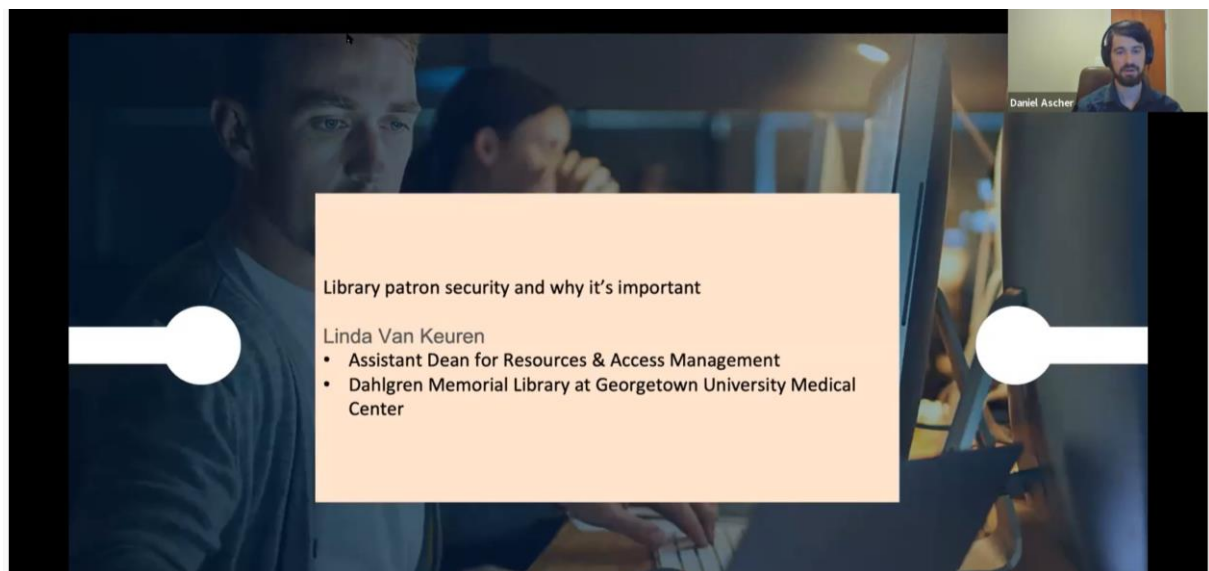
Polling Question 2

How much do you know about the different kinds of cybersecurity threats to the scholarly infrastructure (how peer reviewed literature and open access content is shared, funded and trusted)?

Okere, Kilechi N. (E...)

#ensisecurity2020

1:39:46 4:30:32



A video player interface with a background image of two people working at a computer. A light orange box in the center contains text about a speaker. In the top right corner, there is a small video feed of a man. The bottom of the player shows a progress bar, a play button, and a volume icon.


Library patron security and why it's important

Linda Van Keuren

- Assistant Dean for Resources & Access Management
- Dahlgren Memorial Library at Georgetown University Medical Center

Daniel Ascher

PowerPoint Slide Show - [Library patron security for Elsevier Summit] - PowerPoint




Library patron security and why it's important

Cybersecurity Landscape: Protecting the Scholarly Infrastructure
Scholarly Networks Security Initiative
October 22 2020

Linda Van Keuren,
Assistant Dean for Resources and Access Management
Dahlgren Memorial Library, Georgetown University Medical Center

Slide 1 of 9

PowerPoint Slide Show - [Library patron security for Elsevier Summit] - PowerPoint



Patron security

- Credentials
- Institutional networks
- Personally identifiable information and confidentially
- Intellectual property

Slide 2 of 9

PowerPoint Slide Show - [Library patron security for Elsevier Summit] - PowerPoint

Linda Van Keulen

Minimizing risks


- Easy access
- Collaborate
- Educate
- Policies
- Federated authentication

Slide 3 of 9

PowerPoint Slide Show - [Library patron security for Elsevier Summit] - PowerPoint

Linda Van Keulen

DML case study



Dahlgren Memorial Library (DML)

- Graduate Health and Life Sciences Research Library at Georgetown University Medical Center
- 99.9% online collections
- Serves the 6,500 FTE of Schools of Medicine, Nursing, Biomedicine, a Cancer Center and Hospital

Slide 4 of 9

PowerPoint Slide Show - [Library patron security for Elsevier Summit] - PowerPoint

Linda Van Keulen

Federated authentication

- 5 years ago - IP based authentication for library resources
 - Security concerns
 - Acquisitions model
 - Minimal statistics
 - Hospital access

Slide 5 of 9

PowerPoint Slide Show - [Library patron security for Elsevier Summit] - PowerPoint

Linda Van Keulen

Federated authentication

- Created logic
- Added attribute
- Configured connection
- Provisioned resources
- Contacted publishers
- Updated URLs

Slide 6 of 9

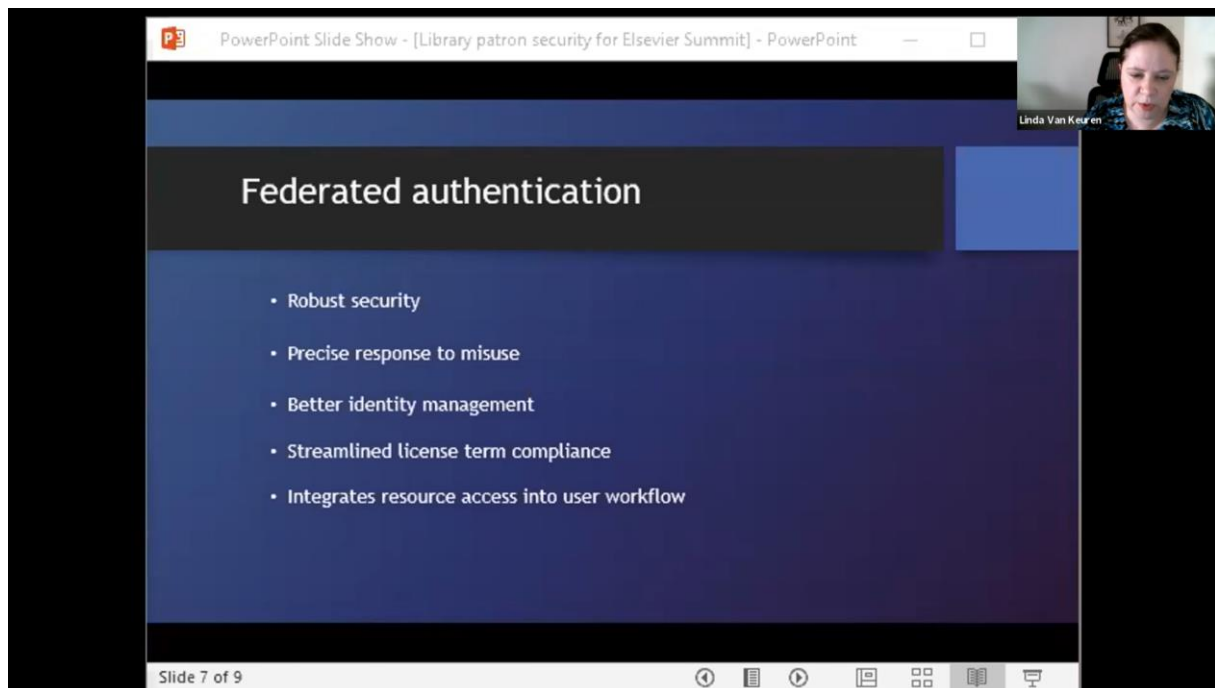
PowerPoint Slide Show - [Library patron security for Elsevier Summit] - PowerPoint

Linda Van Keuren

Federated authentication

- Robust security
- Precise response to misuse
- Better identity management
- Streamlined license term compliance
- Integrates resource access into user workflow

Slide 7 of 9



PowerPoint Slide Show - [Library patron security for Elsevier Summit] - PowerPoint

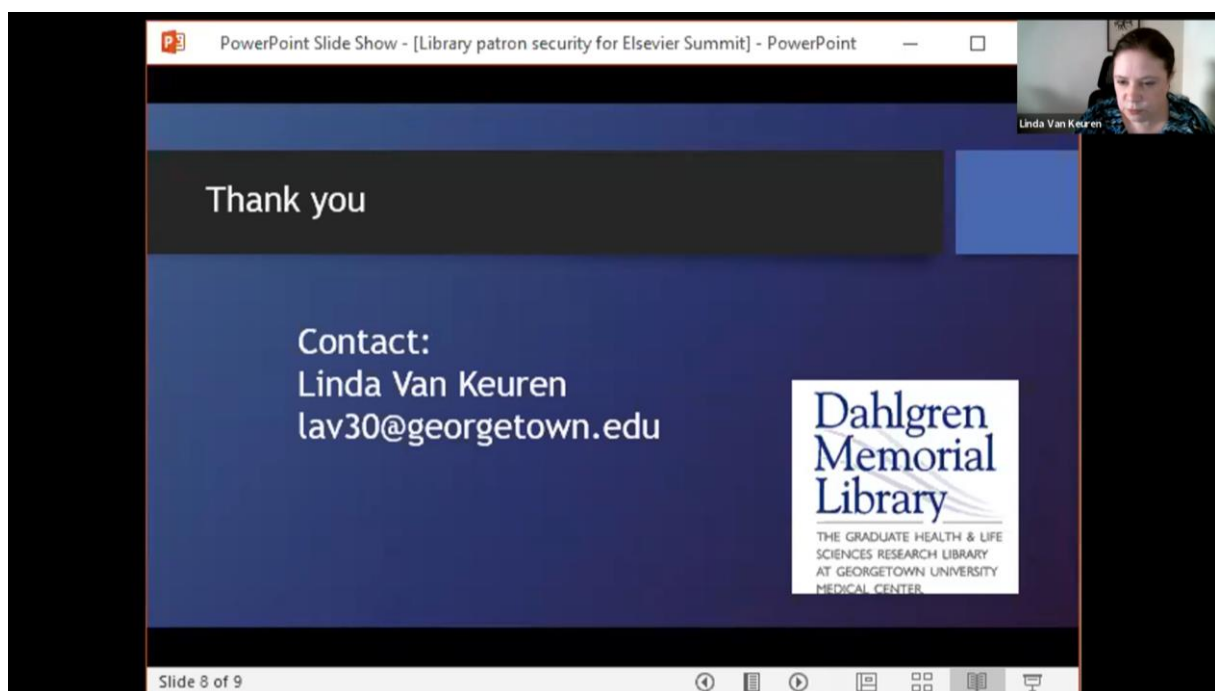
Linda Van Keuren

Thank you

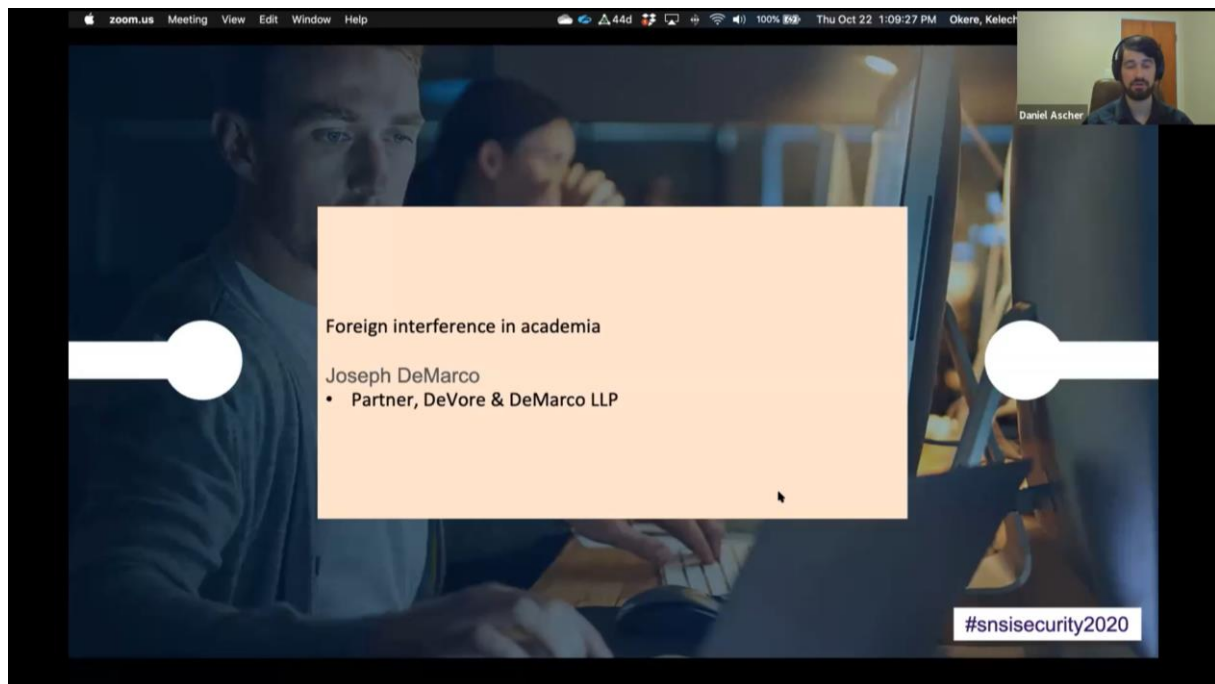
Contact:
Linda Van Keuren
lav30@georgetown.edu

**Dahlgren
Memorial
Library**
THE GRADUATE HEALTH & LIFE
SCIENCES RESEARCH LIBRARY
AT GEORGETOWN UNIVERSITY
MEDICAL CENTER

Slide 8 of 9



zoom.us Meeting View Edit Window Help 44d 100% Thu Oct 22 1:09:27 PM Okere, Kelech



Foreign interference in academia

Joseph DeMarco

- Partner, DeVore & DeMarco LLP

#snsisecurity2020

Daniel Ascher