BACKGROUND AND METHODOLOGY
The brief
The Scholarly Networks Security Initiative (SNSI) wanted to understand what academic librarians understood about cybercrime and what their main concerns were. They particularly wanted insights on what the librarian community thought about illegal websites that offer access to scholarly resources that would normally be accessed from publishers’ platforms.

The approach
Shift developed a survey in collaboration with SNSI. The survey was disseminated via a combination of data suppliers, data from SNSI members and Shift’s own lists, which allowed Shift to reach respondents from around the world. As part of the survey, academic librarians were shown a range of statements and asked to rate how much they agreed with each one. In the analysis stage this revealed librarian attitudes towards illegal websites that offer access to scholarly resources.

The value
The report and presentation were shown to SNSI members, including large and small publishers, learned societies and university presses, and others involved in scholarly communications. The findings grew their understanding of how best to support librarians with cybercrime, and how to tailor communication to different groups.
There were 278 usable responses to the survey.

Profile of respondents

**Job role**
- Librarian: 94%
- Other roles: 6%

**Institution size**
- Small: 26%
- Medium: 29%
- Large: 44%

**Institution type**
- University: 86%
- Other higher or further education establishment: 14%

**Continent**
- North America: 57%
- Europe: 29%
- Asia: 6%
- Other continents: 3%

**Age**
- 18-34: 15%
- 35-54: 53%
- 55-74: 30%
- Prefer not to say: 3%

Base n: 278

©SHIFT INSIGHT 2021
UNDERSTANDING AND CONCERNS AROUND CYBERCRIME & DATA SECURITY
Most reported having some understanding of cybercrime and data-security issues

- Reluctance to say expert or no understanding.
- Large higher education institutions more likely to say ‘expert’.
- Least confidence around ransomware and remote learning privacy

Q: How well would you say you understand these issues around cybercrime and data-security?

<table>
<thead>
<tr>
<th>Issue</th>
<th>None</th>
<th>Little Understanding</th>
<th>Some Understanding</th>
<th>High Level Understanding</th>
<th>Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses</td>
<td>1%</td>
<td>11%</td>
<td>33%</td>
<td>54%</td>
<td>1%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>1%</td>
<td>3%</td>
<td>18%</td>
<td>22%</td>
<td>56%</td>
</tr>
<tr>
<td>Data theft</td>
<td>1%</td>
<td>2%</td>
<td>12%</td>
<td>35%</td>
<td>49%</td>
</tr>
<tr>
<td>Remote learning privacy concerns</td>
<td>4%</td>
<td>15%</td>
<td>24%</td>
<td>54%</td>
<td>1%</td>
</tr>
<tr>
<td>Staff using personal devices</td>
<td>2%</td>
<td>17%</td>
<td>29%</td>
<td>49%</td>
<td>2%</td>
</tr>
</tbody>
</table>
45% of respondents said they had a high level of understanding around issues surrounding login sharing.

Q: How well would you say you understand these issues around cybercrime and data-security?

- Students making their university network logins available to others:
  - None: 2%, Little understanding: 10%, Some understanding: 40%, High level understanding: 45%

- Student/staff personal data being stolen:
  - None: 2%, Little understanding: 12%, Some understanding: 35%, High level understanding: 49%

- Phishing:
  - None: 1%, Little understanding: 8%, Some understanding: 44%, High level understanding: 46%

- More likely to have confidence in their understanding of:
  - phishing.
  - students making their university network logins available to others.
  - student/staff personal data being stolen.

- North America – higher confidence

- Respondents felt relatively confident in their understanding of student login sharing in relation to data-security risk.
Security of staff/student data and reputational damage were top concerns.

Q: In your professional life, what concerns you most? (open Q)

- Protecting staff and student data was the top concern.
- Even more concern around this area in the USA than Europe.
- Fear of damage to reputation, increased work-load, preventing students from learning.
- The more they felt they knew, the more concern they had.

- Protecting research data: 2%
- Phishing emails: 4%
- Cyber-attacks preventing learning: 4%
- Lack of protective measures: 8%
- Impact on workload: 7%
- Ransomware: 9%
- Identity theft: 9%
- Loss of data or control over systems: 11%
- Nothing: 18%
- A reputationally damaging cyber-attack: 18%
- Security of staff and student data: 37%

Base n: 278
Base n European librarians: 81; base n US librarians: 149
Theft of staff and student personal data concerned them most.

How much do you feel these are concerns for your library?

- Staff / student personal data theft: 15% Unsure, 18% Not a concern, 65% A concern
- Sharing of uni login details: 20% Unsure, 19% Not a concern, 56% A concern
- Phishing emails: 23% Unsure, 20% Not a concern, 55% A concern
- Viruses: 22% Unsure, 24% Not a concern, 54% A concern
- Ransomware: 28% Unsure, 21% Not a concern, 46% A concern
- Zoom-bombing: 27% Unsure, 24% Not a concern, 43% A concern
- Staff using personal devices: 27% Unsure, 25% Not a concern, 41% A concern

• Concern was high for personal data theft and students making their network login details available online.
• Personal data theft concerns high in North America and at larger institutions.
• For ‘experts’, there was more worry over ransomware and viruses.
CURRENT SUPPORT FOR CYBERCRIME & DATA SECURITY
The IT department was the first port of call for most

Q: If you suspected your institution’s network had been compromised, how likely would you be to:

- 96% would contact their IT department.
- Highly likely to report to their institution’s security department or tell other librarians.
- Consistent across continents, age groups and institution types.
- Least likely to discuss with students or add to security breach log.

Contact the IT department: 96%
Report to my institution’s security department: 85%
Tell other librarians about the suspected network breach: 85%
Take direct action to restore network integrity: 67%
Report to the CIO or CISO: 59%
Discuss with students how to prevent future network breaches: 43%
Add it to a security breach log: 25%

Base n: 210-260
ILLEGAL SITES
There was uncertainty around illegal websites that offer access to scholarly resources

Are you familiar with any illegal websites that offer access to scholarly resources that would normally be accessed from publishers’ platforms?

- 21% were unsure if they were familiar with illegal websites.
- Most popular answer was Sci-Hub.
- Other answers included legal websites and OA journals.

Can you name any examples?

- Sci-Hub: 63%
- ResearchGate: 25%
- Academia.edu: 12%
- Library Genesis: 10%
- OA Journals: 8%
- DOAJ: 7%
- Google Scholar: 4%
- Unpaywall: 4%
- ICanHazPDF: 3%
- Research for Life: 2%
- Openstax: 2%
- Other: 1%

Familiarity base n = 278, Naming example base n = 172
Librarians have complex attitudes towards these resources

Q: To what extent do you agree with the following statements with regard to sites such as Sci-Hub

<table>
<thead>
<tr>
<th>Statement</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Not sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>It's fine for librarians to point a learner to these sources if a paper</td>
<td>64%</td>
<td>14%</td>
<td>13%</td>
<td>8%</td>
</tr>
<tr>
<td>is not available at their institution</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free public access to research should be a legal right</td>
<td>66%</td>
<td></td>
<td>18%</td>
<td>9%</td>
</tr>
<tr>
<td>Using these sites is wrong</td>
<td>45%</td>
<td></td>
<td>28%</td>
<td>11%</td>
</tr>
<tr>
<td>Sources like these are useful to learners</td>
<td>47%</td>
<td></td>
<td>26%</td>
<td>10%</td>
</tr>
</tbody>
</table>

- Respondents agreed that it shouldn't be used and wouldn't recommend it, but they agreed with some of the principles on which it claims legitimacy.
- The age group 18-34 were more sympathetic to Sci-Hub.
Respondents saw Sci-Hub as a threat to their institution’s network, but were still sympathetic to some of its values.

To what extent do you agree with the following statements with regard to sites such as Sci-Hub:

- I worry that sites like this may have access to my institution’s networks
  - 18% Disagree
  - 18% Neutral
  - 21% Agree
  - 43% Unsure

- Students using sites such as this puts my institution’s network at risk...
  - 23% Disagree
  - 14% Neutral
  - 21% Agree
  - 42% Unsure

- Just because these sites are illegal doesn’t mean that they are wrong...
  - 9% Disagree
  - 38% Neutral
  - 27% Agree
  - 26% Unsure

- Sites like these are breaking copyright law and should be prosecuted...
  - 12% Disagree
  - 13% Neutral
  - 28% Agree
  - 47% Unsure

- These sites are bad for publishers but good for learning
  - 12% Disagree
  - 15% Neutral
  - 27% Agree
  - 46% Unsure

- Respondents were concerned with Sci-Hub from a data-security perspective.

- There was a gap in understanding about risk to institutions’ networks through Sci-Hub.

- And a lack of agreement on ethics
CONCLUSIONS
Conclusions

- Respondents had limited confidence around cybersecurity.

- They were mostly concerned with data protection and ensuring that their colleagues, students and institutions were safe.

- Librarians main areas of concern around cybersecurity were personal data and reputational risk.

- Attitudes to Sci-Hub were complex.