Scholarly Networks Security Initiative

Certified B Corporation

SHIFT INSIGHT

SNSI cybersecurity and academic libraries

Authors – Caroline Wheeler, Georgia Woollett & Andy Dzro

WWW.SHIFT-INSIGHT.CO.UK

Glossary of terms 3

Executive summary 8

Background and research objectives 12

Profile of respondents 14

Understanding and concerns around cybercrime and data security 17

Concerns relating to the library 25

Mitigating security risks 27

Awareness and views around AI, pirate sites and research integrity 33

Conclusions and recommendations 49

Glossary of terms

Glossary

Term	Definition
Central Authentication Service (CAS)	A single sign-on protocol that allows users to access multiple web applications after logging in just once.
Chief Information Security Officer (CISO)	A senior-level executive responsible for establishing and maintaining an organisation's information security strategy.
Cyber Hygiene	The set of practices and procedures used by individuals and organisations to maintain the security and health of their digital systems, devices and data.
Data Loss Prevention	A security solution that identifies and prevents the unsafe or inappropriate sharing of sensitive data to protect against breaches and exfiltration.
Disaster Recovery	The process of an organisation using pre-defined plans and procedures to restore its IT infrastructure and operations after a catastrophic event, such as a natural disaster, cyberattack or hardware failure.
Doxware	A form of malicious software. It enables hackers to steal data so they can threaten to leak sensitive personal information.
Endpoint Detection	A cybersecurity approach that continuously monitors endpoints like laptops, desktops and mobile devices to detect, investigate and respond to cyber threats in real-time.
Endpoint protections	The practice of securing devices like laptops, smartphones and desktops that connect to a network, using cybersecurity solutions to defend against threats such as malware and data breaches.
Geo-blocking	The practice of restricting access to online content based on a user's geographic location, often using their IP address to determine their location.

Glossary

Term	Definition
Identity Access Management Frameworks	A system of policies, processes and technologies that manages digital identities and controls who can access an organisation's data and resources.
Intellectual property (IP)	Creations of the mind, such as inventions, literary and artistic works, designs, symbols, names and images used in commerce.
Large Language Models (LLM)	A software tool capable of corpus-based linguistic analysis and prediction, particularly an artificial intelligence system that processes written instructions (prompts) and can generate natural language text.
Learning Management System (LMS)	A software application or online platform used to administer, document, track, report on and deliver educational courses and training programmes.
Legacy System Upgrades	Modernising outdated software and infrastructure to improve performance, security and efficiency.
Lightweight Directory Access Protocol (LDAP)	A standard application protocol for accessing and managing information services in a distributed directory.
Malware	Software that is specifically designed to disrupt, damage or gain unauthorised access to a computer system.
Multi-factor Authentication (MFA)	A security process that requires users to provide two or more verification factors to gain access to a system, account or application.
Nation-state attacks	Cyberattacks carried out by a government-sponsored group against another government, organisation or individual, for intelligence, espionage or to cause disruption.

Glossary

Term	Definition
NIS2	A unified legal framework to uphold cybersecurity in 18 critical sectors across the EU.
OAuth2	An open standard for authorisation that allows a user to grant a third-party application limited access to their data on another service, without sharing their password.
Phishing attack	A type of cyberattack where attackers impersonate trusted sources to trick people into revealing sensitive information like passwords, credit card numbers and bank details.
Pirate site	An online platform that provides unauthorised access to copyrighted material like movies, music, software or books without permission.
Ransomware	A type of malware which prevents users from accessing their device and the data stored on it, usually by encrypting files.
Role-based access controls	A system that restricts system access to authorised users based on their role within an organisation, rather than assigning permissions to individuals.
Shadow Library	An illegal online repository that provides free access to copyrighted digital content, such as academic papers and e-books, that is normally behind access controls or otherwise not accessible without a fee.
Single Sign-On (SSO)	An authentication method that lets users log in to multiple applications and services with a single set of credentials.
SIP2	An international protocol for exchanging messages between vending machines and library systems.
The Higher Education Technology Agenda (THETA)	A biennial conference that aims to advance higher education and research by promoting the intelligent use of information technology.

Glossary

Term	Definition
Third party vendor compromise	A cybersecurity attack where attackers gain access to a company's sensitive information or systems by breaching a trusted third-party vendor, such as a supplier, service provider or contractor.
Virtual Private Network (VPN)	An arrangement whereby a secure, apparently private network is achieved using encryption over a public network, typically the internet.

Executive summary

Executive summary

Shift Insight conducted an international survey with **287 librarians** and **20 interviews** with Chief Information Security Officers (CISOs) to understand their views and priorities around cybersecurity.

Level of perceived cybersecurity risk in the university sector

- In 2025, **85% of librarians agreed that cybersecurity threats are increasing, consistent with Chief Information Security Officers CISO views**. Compared to 2021 and 2022, the perceived risk has intensified, and universities were considered prime targets for cyber attacks, because they hold large volumes of valuable data, including student information, research and intellectual property. This was coupled with outdated systems and limited funding, which exposed institutions to increasingly sophisticated attacks including AI-driven threats.
- **Awareness and understanding of cybercrime and data-security issues among staff and students is mixed.** CISOs noted students were a weak link due to low engagement and poor cyber hygiene. Librarians showed strong awareness – 93% reported at least some understanding, an improvement from 2021.
- **The most common breaches included phishing attacks, ransomware, financial fraud and third-party vendor compromises.** A smaller number of CISOs and librarians also mentioned threats from nation state actors.
- CISOs are mainly investing in Multi-Factor Authentication (MFA), identity access management frameworks, endpoint detection and response, AI governance, data loss prevention, disaster recovery, legacy system upgrades. Some are signing up to directives like NIS2 in the EU.

Library related security risks

- **44% of librarians saw security risks arising from the library as equal to other departments**; 28% saw it as higher, citing third-party vendors and sensitive data. Most CISOs viewed libraries as low-risk due to strong collaboration and tech-savvy staff.
- There was awareness of Intellectual Property (IP) theft from library systems among CISOs. Several CISOs reported incidents of mass journal downloads via compromised credentials at their institutions.

Executive summary

Awareness of Sci-Hub and similar piracy sites

- **Awareness of Sci-Hub among librarians remained stable** (69% in 2025 vs. 63% in 2021). Awareness of LibGen and Z Library has increased since 2021. Confusion persists around the legality of content sharing sites.
- Librarians and CISOs learned about pirate sites via word of mouth, listservs, peer networks and students.
- **Librarians estimated low usage of Sci-Hub – over a third said under 20% of faculty and students use Sci-Hub**, with 34% unsure. CISOs working in regions with well-funded libraries also believed usage was low. In contrast, a CISO in Ethiopia reported widespread use of Sci-Hub to access journals that the university does not subscribe to.

Research integrity and pirated content

- **Librarians were split: 45% saw pirate sites as a risk to research integrity, while 43% saw them as useful for learners.** 52% considered them to be bad for publishers, but good for learning. These findings should be placed in the context that most librarians agreed public access to research should be free (76%). Concerns about LLMs being trained on pirated content were high (71% believed this and 95% concerned).
- **Half of librarians expressed concern about protecting research data and university IP**, such as patents.

Executive summary

User authentication and ‘know your customer’

- Librarians and CISOs have a number of steps in place to establish that system users are who they say they are. CISOs and librarians use MFA, SSO, geo-blocking, and role-based access controls to verify users. These measures are essential to prevent credential abuse and ensure secure access to library systems.

Collaboration between CISOs and librarians

- Both groups advocated for joint risk assessments, regular communication, shared training and inclusion of librarians in policy development and governance.

Background and research objectives

Background and methodology

Background

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, university presses and others involved in scholarly communications.

SNSI were looking to repeat previous research run in 2021/22 into university cybersecurity awareness. Previously, the research was conducted in two parts – a quantitative survey with university librarians in 2021, followed by a qualitative interview phase with institution Chief Information Security Officers (CISOs) in 2022. In this iteration, they wanted a single, unified project.

Methodology

Qualitative interviews with CISOs

- **20 online interviews** were conducted with CISOs internationally.
- Interviews lasted 45 minutes each and were conducted over Microsoft Teams.
- Interview participants received an incentive payment of £150 or equivalent in their local currency.

Quantitative eSurvey with Librarians

- SNSI and Shift collaboratively designed a survey for university librarians.
- The survey was disseminated through Shift and SNSI panels, listservs and social media.
- Shift processed the survey data and cleaned unusable responses. The final sample had **287 responses**.

Profile of respondents

Profile of interview participants

Institution type

University – 19

Other – 1

Job title

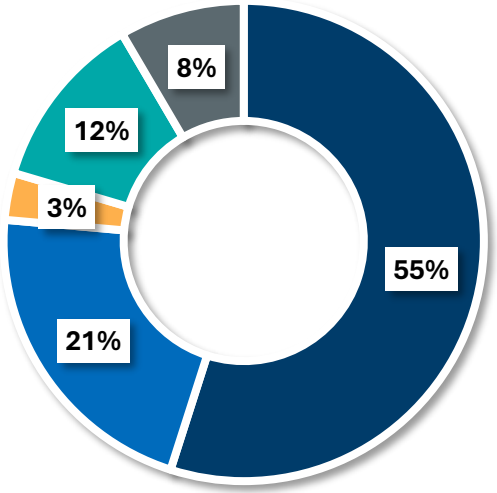
Chief Information Security Officer	5
Chief Information Officer	4
Director/Head of IT	4
Information Security Officer	3
Chief Executive Officer	2
Director of Risk and Assurance	1
Director of Cyber Security	1

Country

United states of America	5
Australia	4
United Kingdom	4
Netherlands	2
Brazil	1
France	1
Ethiopia	1
Germany	1
South Africa	1

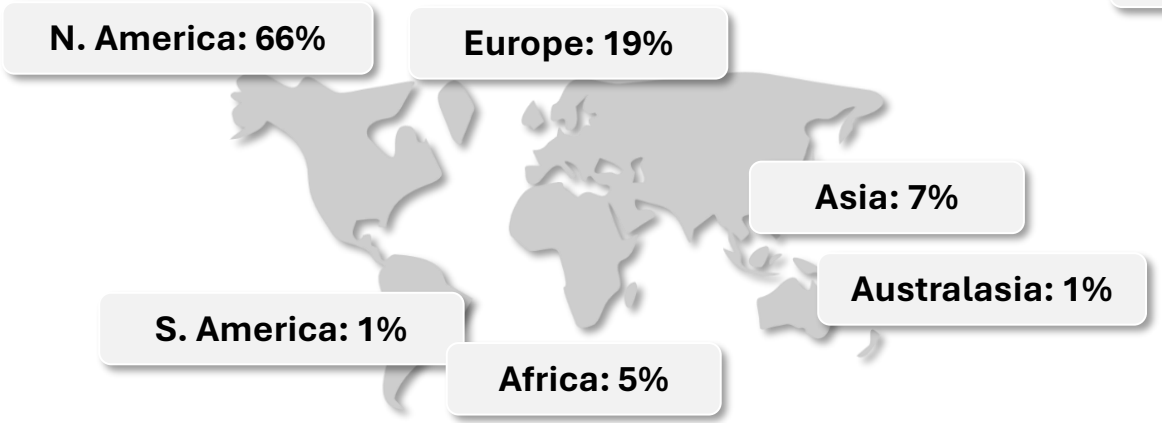
Profile of survey respondents

Job role

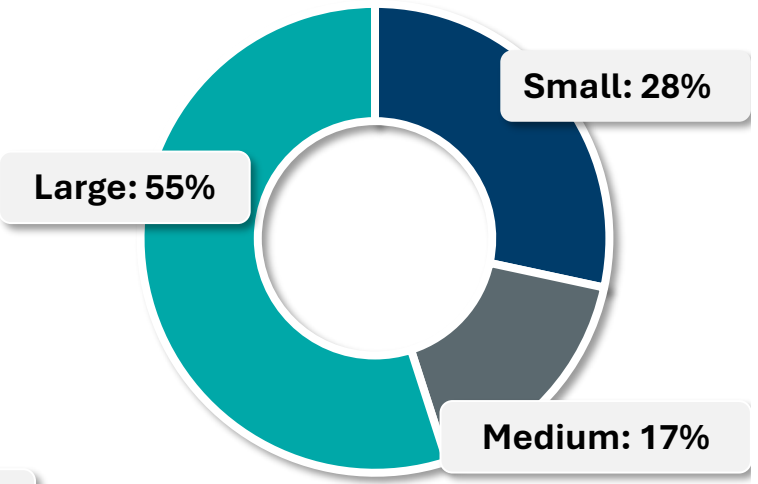


- Librarian
- Library manager or administrator
- Dean of Libraries
- Acquisition / subject librarian
- Other role within an academic library

Continent



Institution size

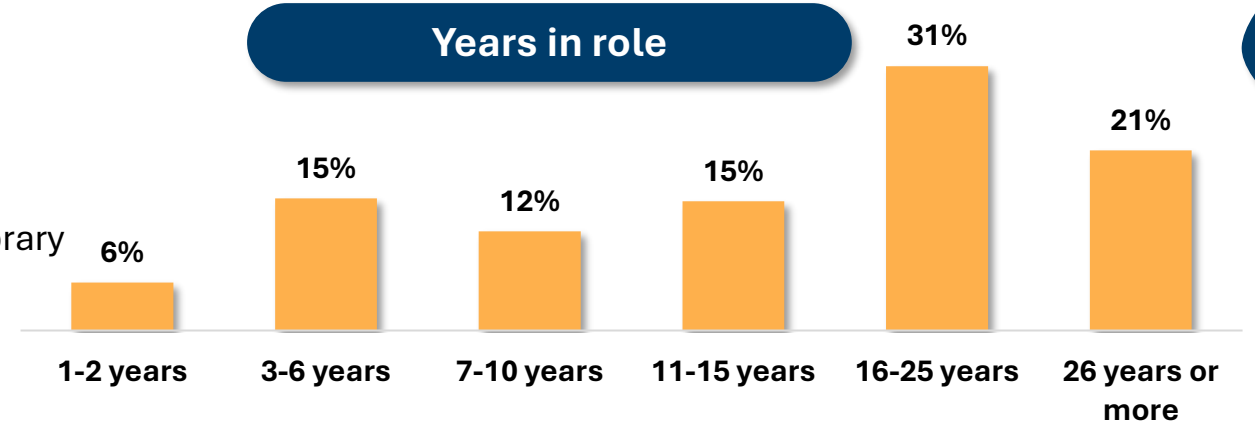


Institution type

University – 88%

Other higher or further education establishment – 10%

Years in role



Base n = 284.

Understanding and concerns around cybercrime and data security

The level of perceived cybersecurity risk in the higher education sector remained high

As in 2022, **CISOs felt that the level of cybersecurity risk in the higher education (HE) sector was high and that this risk was increasing. This sentiment was also held by librarians**, 85% agreed that cybersecurity threats were on the rise for universities, while only 2% disagreed.

CISOs identified several factors contributing to this elevated and growing risk. **The most commonly mentioned were:**

- Universities are prime targets for cyber attacks as they hold large volumes of valuable data, including student information, research and intellectual property.
- A lack of updated systems, limited funding, and (historically) low senior-level concern cause weakened security controls in HE. Some CISOs reported that awareness at a senior level has increased in recent years, due to increased concerns and reported incidents.
- Universities' open and collaborative environment – combined with widespread use of unmanaged devices by students and staff with varying cybersecurity awareness – greatly increases risk.
- Greater sophistication and frequency of attacks, due to developments in AI.
- Increased activity from nation-state actors, e.g. Russia, Iran, Syria, as well as organised crime.

> *"Oh, it's increased significantly. The stats on that it's gone up something like 300% from some of the last figures. But even more scary is that the success rate has more than doubled. So that not only has the rate gone up, but the success has also gone up ahead of that."*
>
> **Cyber Security Program Director, AUS**

Librarians: Thinking about the higher education sector as a whole, do you think cyber-security threats are on the rise for universities?

Yes: 85% | **No: 2%** | **Unsure: 13%**

Base n = 284.

Institutions are making efforts to improve their users' awareness and understanding of cybercrime

Staff and students

CISOs reported staff and students were often the entry point of cybercrime through social engineering, poor cyber hygiene and insider actions. Interviewees often mentioned instances of staff and students falling victim to phishing attacks, indicating a low awareness of cybersecurity risks at their institution.

Students were seen as a particularly weak link, due to their high turnover and low engagement with IT security. CISOs felt students do not see cybercrime as their concern, being largely focused on their degree. Some mentioned instances of students sharing passwords, using illegal websites, and accessing sensitive data in public spaces.

Staff knowledge is viewed as being generally higher, although this varies by their department and level of seniority. Some CISOs mentioned staff in some research departments don't see themselves a target of cybercrime compared to other higher profile research areas that could be targeted by international hackers. Some noted that researchers with an interest in IT sometimes have higher knowledge.

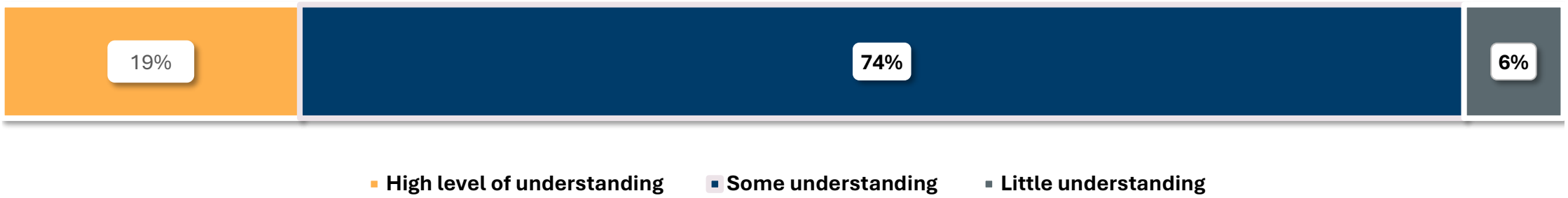
Findings suggest institutions are making efforts to improve staff and student understanding of cybercrime. CISOs interviewed in 2021 mentioned staff were not regularly informed, as there were no mandates to receive cybersecurity training. However, **in 2025, they often mentioned regular communications with staff and students** such as email updates, and that their institution has implemented mandatory annual IT security training for staff and students. Some mentioned implementing efforts to make training more interesting for students to increase engagement.

19% of librarians reported high understanding of cybercrime

CISOs viewed librarians as having a higher cybersecurity understanding due to strong technical foundation for their role. One mentioned librarians at their institution who oversee cybersecurity are 'very attentive and interested' in cybercrime matters.

This is consistent with how librarians self-reported in the survey – **93% stated they had at least some understanding of issues around cybercrime and data security** and less than 1% of respondents reported no understanding.

How well would you say you understand issues around cybercrime and data security?



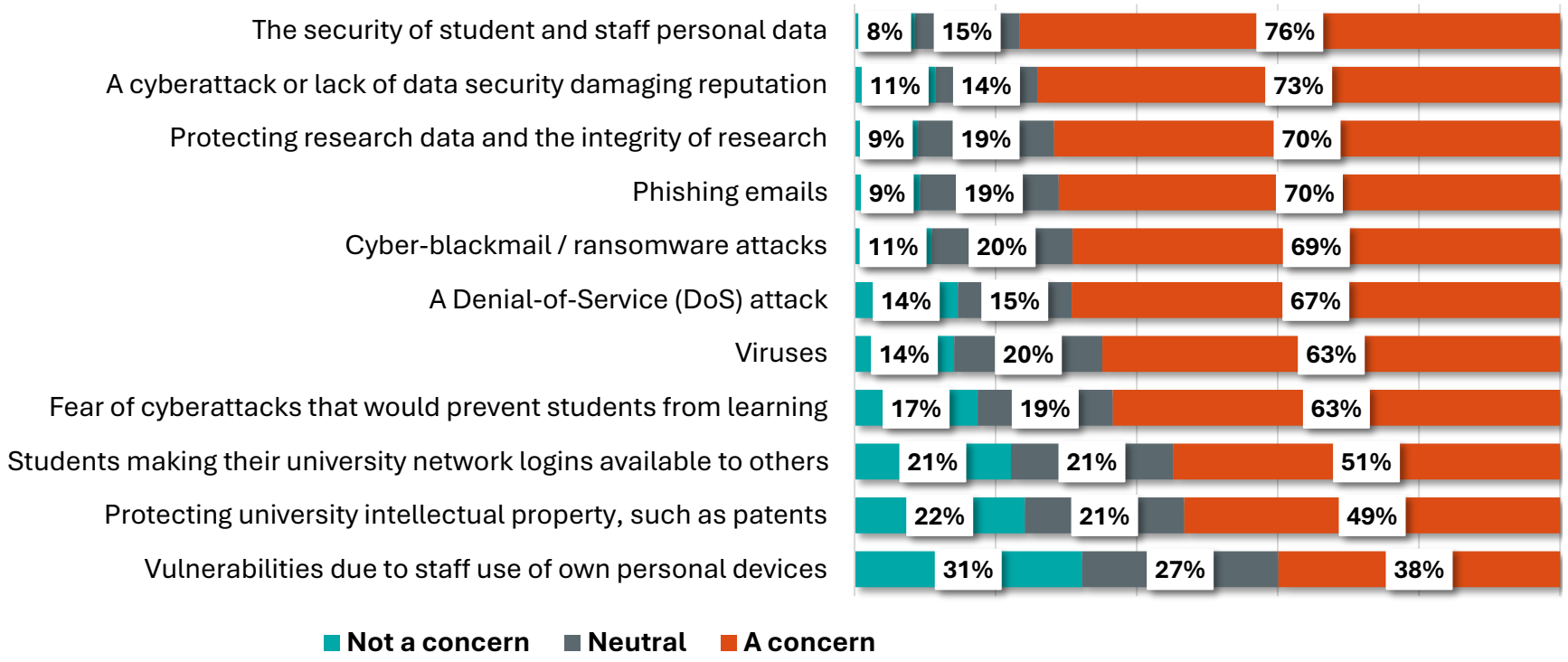
Compared to more experienced respondents, those who had worked in the library sector for less than two years were significantly more likely to report they were unsure how well they understood issues around cybercrime (6%). This suggests they could be a target for increasing awareness.

Base n = 284. Not shown: No understanding <1%), unsure (<1%).

Librarians were most concerned about the security of student and staff personal data

Librarians' most common concern was the security of student and staff personal data (76%), followed by a cyberattack damaging the integrity or reputation of their institution.

In your professional life, how much do you feel these are concerns for your institution's library?



These findings are consistent with attitudes in 2021. In an open question, Librarians were asked what concerns them the most in their professional life. 37% mentioned concerns around security of students and staff personal data.

Base n = 284.

Ransomware attacks were a big concern for CISOs

CISOs mentioned a number of concerns they have relating to cybercrime, data security and related issues. Their biggest and most common concern was ransomware. They felt this poses an existential threat to institutions, due to data theft, operational disruption, potential financial losses and reputational damage. Top concerns are shown below:

Ransomware attacks

- CISOs described this as the top threat that could disrupt campus services.
- They felt it is often linked to other risks such as phishing emails and organised crime.

Phishing attacks and emerging threat of AI

- CISOs frequently mentioned staff and students receiving phishing emails.
- They noted AI spear-phishing and deep-fake technologies are becoming increasingly sophisticated, convincing and difficult to identify – increasing attacker scale and nuance.

Insider risk

- CISOs noted malicious or negligent workflows are a frequent source of unauthorised access and data leakage.
- They felt this is sometimes due to low cybersecurity awareness among staff or students and inadequate security systems (including MFA or SSO) making it easier for other users to gain access.

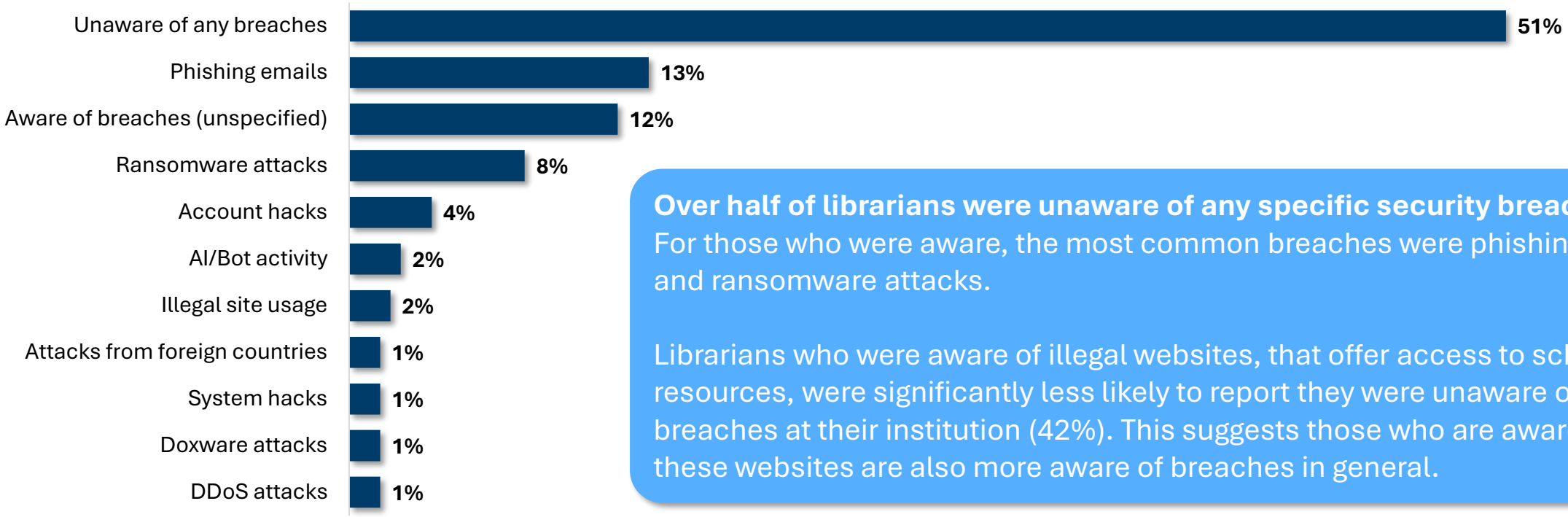
Open, collaborative campus environments

- CISOs were concerned public spaces, terminals and libraries – as well as shared devices – increase risk of attack, in ways which are difficult to monitor and control.
- Some mentioned students signing up to external tools or pirated sites can cause data leakage and exposure to malware.

Phishing emails were the most common cause of security breaches

Librarians were asked if they were aware of any security breaches caused by people using pirated sites at their institution, which we explore later in the report. This was followed by an open question asking if they were aware of any breaches more generally.

Other than Sci-Hub/pirated sites, are you aware of any security breaches due to any other cause at your institution, such as ransomware? (coded open question)



Over half of librarians were unaware of any specific security breaches. For those who were aware, the most common breaches were phishing emails and ransomware attacks.

Librarians who were aware of illegal websites, that offer access to scholarly resources, were significantly less likely to report they were unaware of any breaches at their institution (42%). This suggests those who are aware of these websites are also more aware of breaches in general.

Q23. Base n = 219, not shown: unsure (3%), other (4%), malware attacks (<1%), IT software hacks (<1%).

Breaches experienced by CISOs were a combination of human-factor vulnerabilities and technical flaws

Most CISOs reported a number of cybersecurity breaches at their institution. These included:

- **Phishing emails.** These were identified as the most frequent cybersecurity breach – CISOs noted that many staff and students have received phishing emails.
- **Financial fraud.** Multiple CISOs mentioned instances of fraud, such as payroll redirect attacks, admission fraud to receive a government educational assistance payment, and student identity threat to take out student loans.
- **Multi-factor authentication (MFA) fatigue.** One CISO noted that users have accepted MFA notifications they didn't initiate, leading to bad actors getting into their account.
- **Nation-state targeting.** A member of staff at one institution was targeted by a nation-state backed attacker.
- **VPN vulnerability.** Flawed VPN technology at one institution allowed a bad actor to access an unsecure server.

They also mentioned instances of breaches at other institutions:

- **Ransomware attacks** were commonly mentioned as high-impact security incidents they had heard of at other institutions, leading to an institution-wide shut-down of operations.
- Some had heard of instances of **third-party vendor compromise** at shared vendors leading to multi-institution exposure.

Several CISOs mentioned instances of hackers targeting university libraries to access and download journals, as explored further in the Sci-Hub section.

> *"[Actors] would log into the library and then start downloading, you know, PDFs at a very high rate. We would get an alert, typically from the journal owner… like, hey, did somebody really mean to download 8,000 articles?"*
>
> **Head of IT operations, UK university**

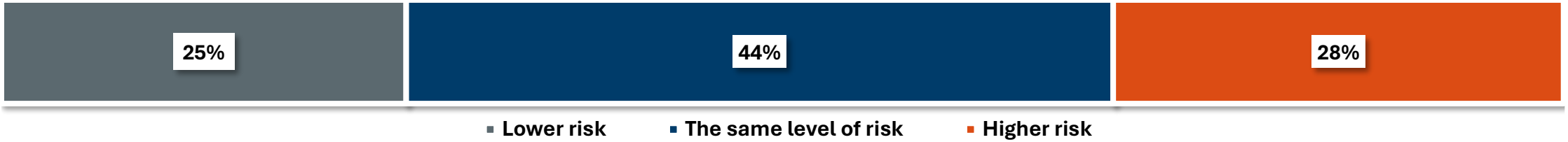
Concerns relating to the library

Almost half of librarians saw cybersecurity risks in libraries as equal to those in other departments

44% of librarians believed that the library faces a similar level of risk as other departments in their institution. When asked to explain their reasoning:

- Among those who perceived the library as lower risk, 44% most frequently attributed this to the fact that they do not handle or store sensitive or personal data.
- Of those who viewed the risk as the same, **19% explained that this was because the same systems are used throughout the institution**. This meant they thought there was the same level of risk and security across all departments.
- For participants who viewed the risk as higher, **24% cited the use of third-party vendors, while 18% pointed to the storage of personal or sensitive data**. This suggests they had a lack of confidence in third-party systems managed outside of the institution.

Compared to other parts of your institution do you think the library is exposed to higher or lower cybersecurity risk?



Base n = 284.

Mitigating security risks

CISOs took a number of approaches to pre-emptively reduce cybersecurity risks

MFA and strong password protection

- Commonly used across institutions to increase security on accounts and reduce credential abuse.
- ID verification is often used for onboarding and password resets to prevent account takeover.

Endpoint protections, antivirus and ransomware-specific tools

- Used to detect and block malicious threats and enable rapid endpoint protection.
- Network perimeter tools are also used to stop malicious sites.

Detection and monitoring

- Institutions run regular vulnerability scanning, patch management and tests to find weaknesses.
- Maintaining documents and logs to keep track of root-causes of threats and post-incident lessons learned.

Behavioral interventions and increasing awareness

- Institutions run mandatory trainings to reduce susceptibility to social engineering.
- Some mentioned using creative audience-specific trainings to increase engagement, such as through gamification and events.

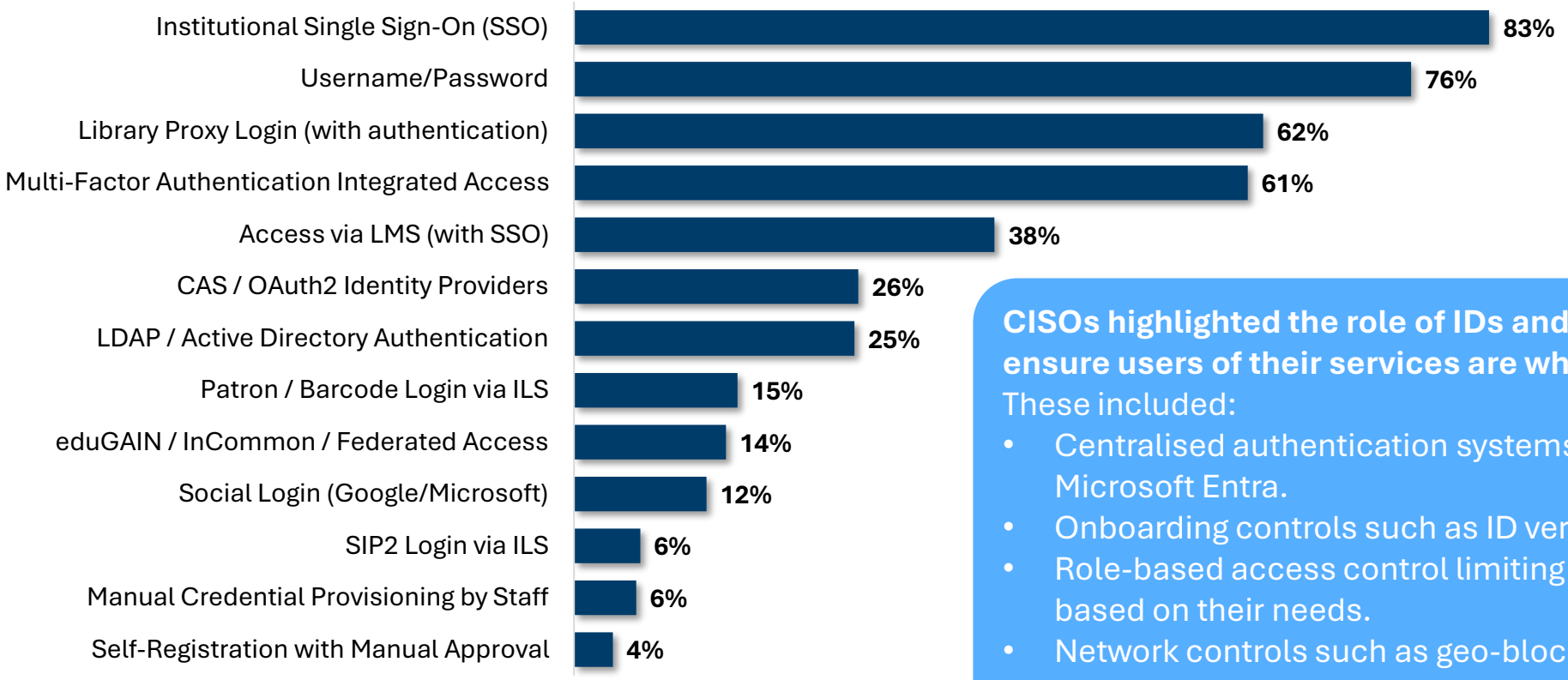
CISOs commonly block certain sites on the network. Those blocked include:

- **Security-focused blocks –** such as malware, phishing and scam sites.
- **Academic integrity/copyright violations –** paper mills and cheating services.
- **Policy blocks –** such as gambling, pornography, gaming or drug-related sites.
- **Government blocks –** to stop traffic from high-risk countries such as Russia.

MFA and SSO were commonly used to control who can access library services

As in 2021, several procedures are used to prevent cybercriminals from accessing their library services and systems.

What procedures do you have in place to ensure the users of your services are who they say they are?



CISOs highlighted the role of IDs and authentication steps to ensure users of their services are who they say they are.
These included:

- Centralised authentication systems such as SSO and Microsoft Entra.
- Onboarding controls such as ID verification.
- Role-based access control limiting what users can access based on their needs.
- Network controls such as geo-blocking as additional verification layers.

Base n = 284.

Cybercrime detection and prevention has improved, but new threats are emerging, including those posed by AI

CISOs interviewed in 2025 indicated that network security measures and cybercrime prevention has improved in the last few years, at their institution and across the HE sector as a whole. This is in part due to the **widespread adoption of multi-factor authentication (MFA) across most systems**, and increased user acceptance of these processes.

Despite improvements, significant challenges remain due to evolving threats, financial and resource constraints at some institutions and human factor vulnerabilities (e.g. credentials sharing) which still persist, even with improved education. Priority security measures which CISOs are investing in now, and in the future include:

- Adoption of endpoint security detection and response (EDR) solutions, such as CrowdStrike.
- Identity and access management (IAM) systems for enhanced authentication.
- Increased cloud platform security and third-party vendor risk monitoring.
- Implementing data loss prevention (DLP), data back-up and disaster recovery procedures to mitigate the impact of future security breaches.
- Modernisation of legacy systems to address vulnerabilities.
- Adoption of security frameworks and standards such as NIS2 in the EU, and 'zero trust' approaches to cybersecurity.

Several CISOs mentioned increased vigilance around the growing use of AI in HE, to understand which AI tools and use cases present a security risk. Strategies included:

- Better governance and policy around the permitted use of AI in the institution.
- Integrating AI topics into security awareness campaigns and dedicated events to educate staff and students about AI and information security.

'You know, cloning of users and organisations, all those things are still around and they're going to be around for a while and AI is going to make all of this worse because it will be able to do things a lot faster.'

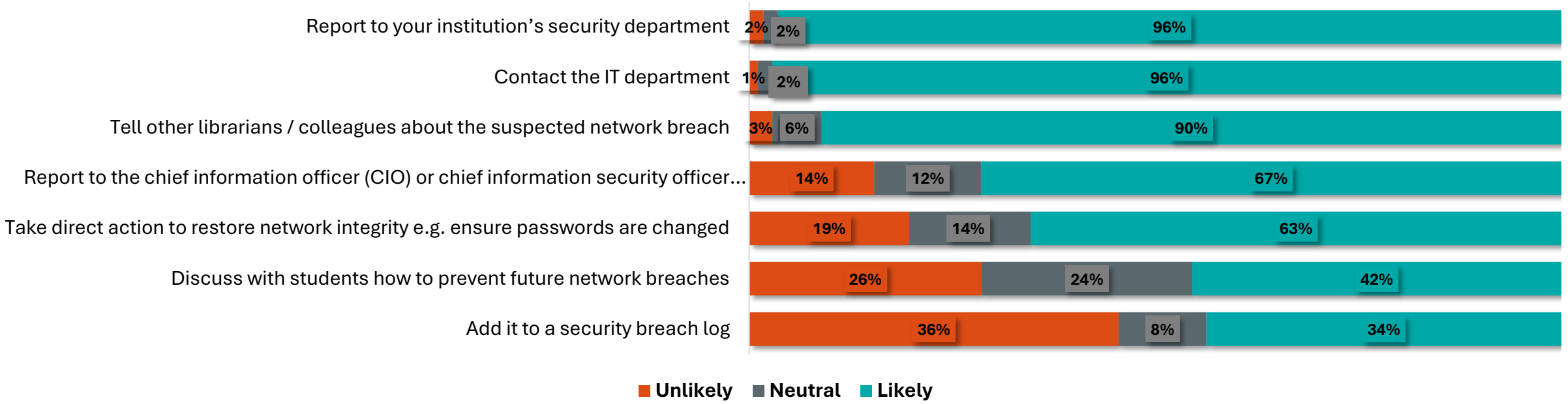
Chief Information Security Officer, State University, USA

So, like everyone else, we are trying to find how far the AI is pushing their boundaries… Sometimes people like any academic independence if it helps in their teaching pedagogy, and they just download [AI tools]. We did a recent scan, and we have 162 AI related tools being used in our institution. With that comes – when people load into tools including ChatGPT, they load our IP, our data. ***We don't know how the data is being used and where it has gone. And also, how that's been affecting the academic integrity.*** *So that's been the biggest threat. So, we're working with academic divisions to identify and educate what AI tools have been approved and what is the key actions and the governance like when we adopt any tools. Before we used to check for privacy and cybersecurity only. So now AI as additional layer of governance has been included.*

Chief Information Officer, University, AUS

96% of librarians would contact their security and IT departments if their network was compromised

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



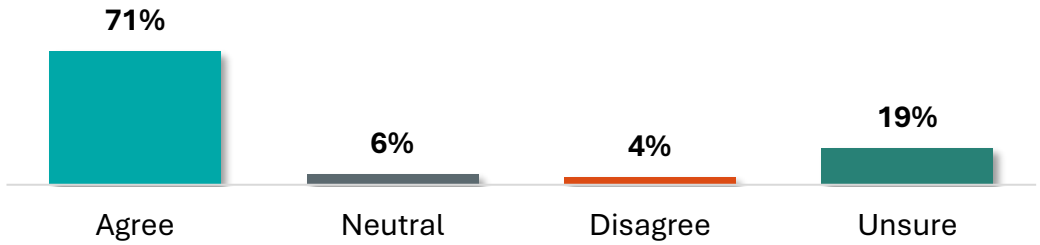
If they suspected their institution's network had been compromised, librarians were most likely to say they would report it to their institution security department and contact their IT department. Similarly, in 2021 96% reported they would contact their IT department, and 85% would report it to their institution's security department. This suggests the steps librarians would take in the event of a network breach have remained consistent since 2021.

Base n = 284 (2025), from 210-260 (2021). Not shown: Report to your institution's security department, unlikely (2%). Contact the IT department , unlikely (1%).

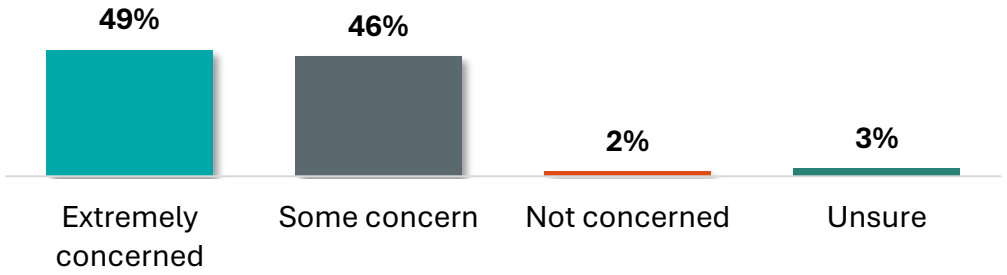
Awareness and views around AI, pirate sites and research integrity

Librarians were very concerned about the implications of LLM models for research integrity

Do you believe that pirated scholarly material is being used to train Large Language Models developed by AI companies?



If this is the case, to what extent are you concerned at the implications of this for research integrity?



Librarians were also asked about concerns around pirated scholarly content being used to train large language models. The implication being that LLM training with pirated materials undermines the integrity of scholarly publishing. It may lead to the dissemination of AI-generated content that lacks proper attribution or verification, potentially eroding trust in academic outputs.

A large proportion (71%) believed this was occurring, and of those, **almost all (95%) expressed concern about its impact on research integrity**.

While CISOs weren't directly asked about pirated scholarly materials in LLM training, they did raise concerns about AI and Sci-Hub activity affecting academic integrity and emphasised the importance of universities controlling their own IP.

'... institutions like universities are mainly called university because of their research material and they own their IP. And that also brings the ranking globally. So if someone accesses it unauthorised, that's a breach of academic integrity as well. So yeah, it's taken seriously'

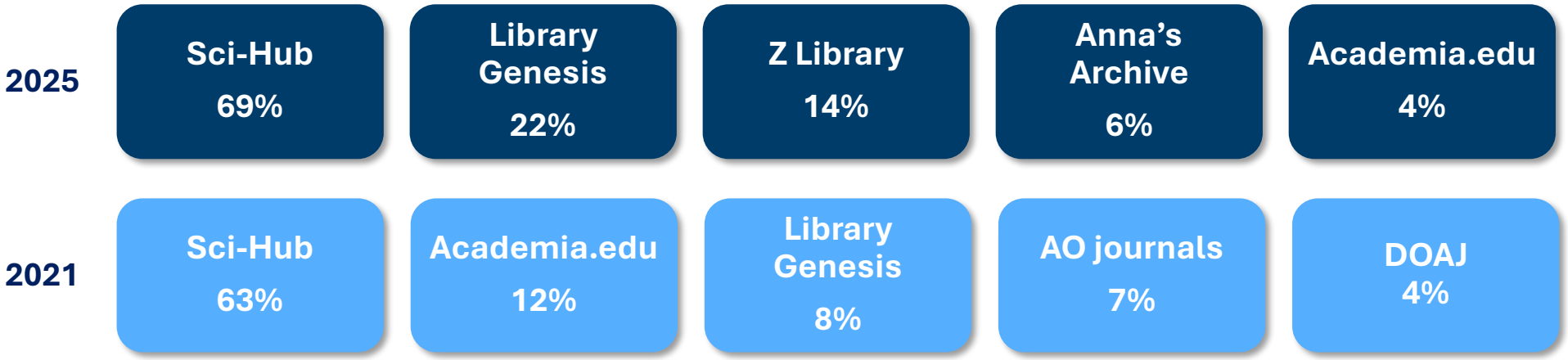
Chief Information Security Officer, AUS

Base n = 284. Combined answer options: agree (strongly agree + moderately agree) and disagree (moderately disagree + strongly disagree)
Base n = 201. Combined answer options: some concern (a little concerned + somewhat concerned)

Over half of librarians were familiar with illegal websites that offer access to scholarly resources

60% of librarians were familiar with illegal websites that offer access to scholarly resources that would normally be accessed from publishers' platforms. 20% were not familiar, and 19% unsure. This is consistent with findings from 2021, where 62% reported they were familiar with illegal websites and 21% were unsure – suggesting awareness has not increased.

Can you name as many examples [of illegal websites] as you can think of?
Coded open question, most common answers from 2025 and 2021 shown:



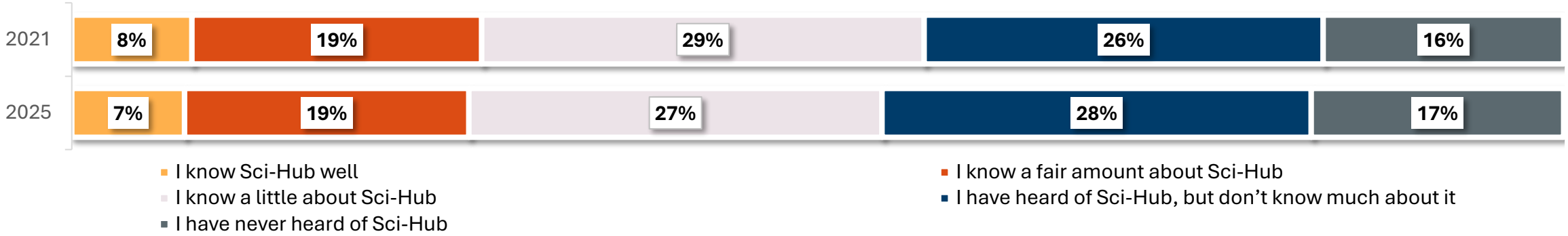
Librarians most commonly listed Sci-Hub (69%), consistent with findings in 2021. Awareness of the 'shadow library' Library Genesis (LibGen) has increased since 2021, alongside Z Library, a similar site.

Base n = 284.
Base n = 139 (2025), 172 (2021).

Librarians' awareness of Sci-Hub has remained consistent since 2021

53% of librarians had some level of familiarity with Sci-Hub, similar to the proportion of CISOs interviewed. 31% of librarians were aware of students or colleagues using Sci-Hub, slightly higher than in 2021.

How familiar are you with Sci-Hub?



Are you aware of any students or colleagues using Sci-Hub or a similar site?

	Yes	No	Unsure
2025	31%	41%	28%
2021	26%	49%	24%

Base n = 284.
Base n = 231.

Librarians at large institutions with more than 10,000 students were significantly more likely to know a fair amount about Sci-Hub (24%). Those who worked at other types of higher or further education institutions were significantly more likely to have never heard of Sci-Hub (35%).

Librarians who reported they know Sci-Hub well were significantly more likely to be familiar with SNSI (30% in 2025, 40% in 2021). This suggests that either campaigns from SNSI may have had an ongoing impact, or those who know of these illegal sites seek out information or initiatives to combat them.

CISOs had mixed awareness of illegal websites – most did not mention Sci-Hub unprompted

Unprompted awareness of Sci-Hub

- Of the 20 CISOs interviewed, only **6** mentioned Sci-Hub unprompted when asked if they were aware of any illegal websites used to access scholarly resources.
- Similarly, only 2 out of 11 CISOs interviewed in 2022 mentioned Sci-Hub unprompted.
- One 2025 participant who was not aware of Sci-Hub mentioned Pirate Bay and Scribd unprompted.

Prompted awareness of Sci-Hub

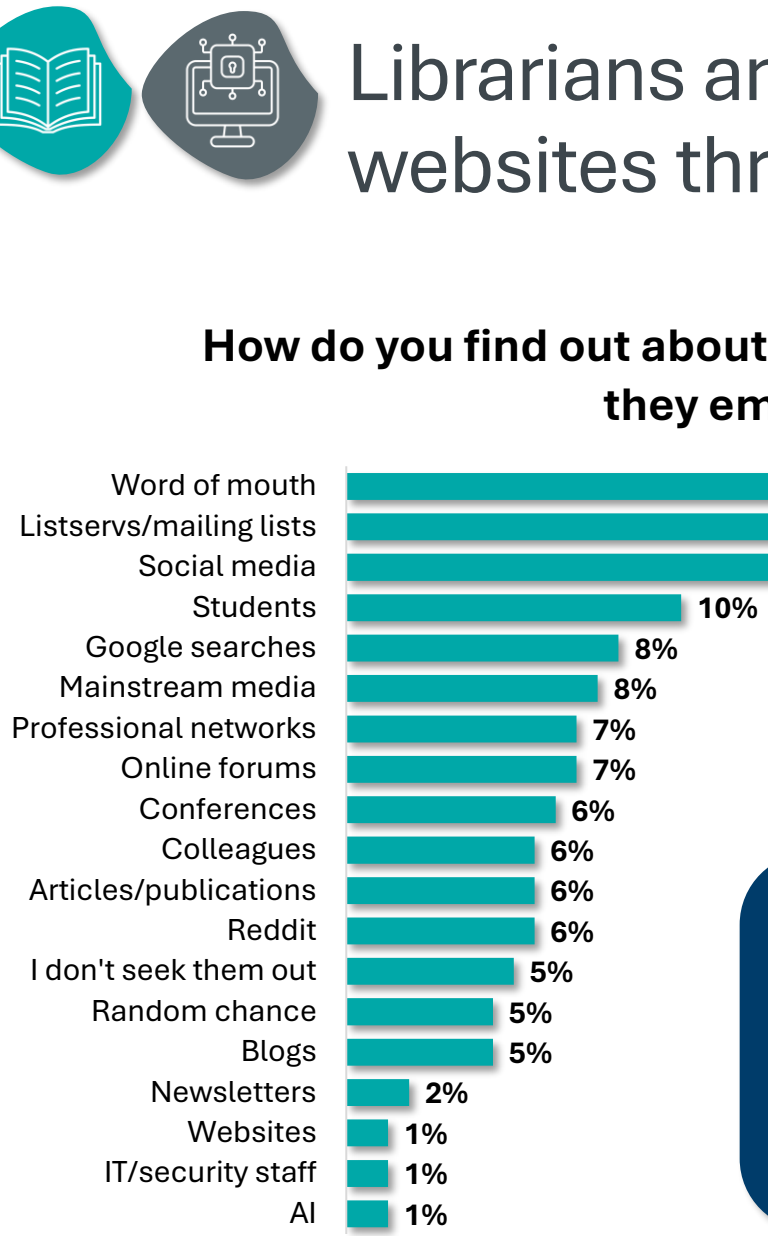
- Once prompted, **11** out of the 20 participants said they had heard of Sci-Hub.

Despite mixed awareness of Sci-Hub, two CISOs mentioned specific security incidents where students' credentials were compromised, which they suspect was due to Sci-Hub activity.

"I haven't heard of like, you know, a major security incident, but we did (and this has fallen off), but for a while we were tracking what I assume was Sci-Hub, who would compromise credentials. I don't know if people were intentionally sharing them, but they seemed like they were compromised credentials."

CISO, US university

Librarians and CISOs commonly heard about new illegal websites through word of mouth



While there were no other significant differences between groups, librarians who had been working in the library sector for over 16 years were significantly more likely to find out through listservs or mailing lists than other methods (45%).

In interviews, CISOs often mentioned hearing about new illegal websites through students or staff, security incidents, regulatory lists and peer networks.

"Just through information sharing amongst the community. You know, people are fairly quick to share that sort of information. They're not so quick to share if they've been breached, but the malicious side of things, that does get well shared."

Head of IT operations, UK university

Base n = 154. Not shown: researchers (<1%), online (<1%), sector news sites (<1%), other (<1%).

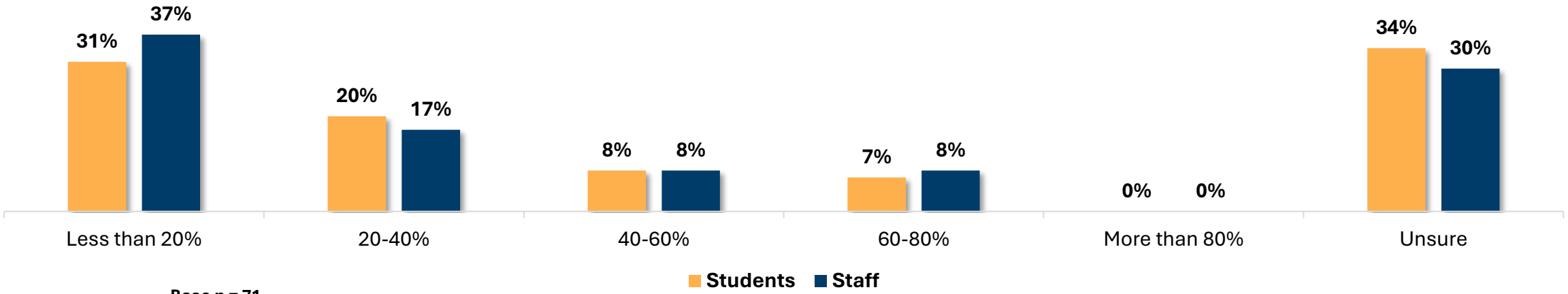
Librarians believed Sci-Hub usage among students and staff was low, or were uncertain about how widely it was used.

Librarians' estimates of Sci-Hub use by faculty and students at their institution were relatively low. **Over a third estimated that fewer than 20% of faculty and students use Sci-Hub.** Interestingly, a large proportion said they were unsure about the extent of its use. This uncertainty may arise as Sci-Hub is often not openly discussed, due to its controversial status.

While research evidence on current usage of Sci-Hub is inconsistent, Walters (2025) suggests that pirate sites are used by 'a substantial minority of university faculty worldwide' with estimates ranging from 25 to 65%.

These findings suggest that Sci-Hub use is an area where understanding continues to develop across academic settings, and that our survey estimates may offer an indicative rather than definitive view of global usage, supporting the case for further research.

What % of your faculty/students would you estimate are using Sci-Hub or other pirating sites to access academic content?



Base n = 71.

Similarly, CISOs working in well-funded institutions thought Sci-Hub use was low

While CISOs were moderately aware of pirate sites like Sci-Hub, monitoring usage was limited. Estimates of usage varied among participants, depending on region. **When asked what percentage of students they thought were using illegal sites, those from Australia and the UK felt this would be below 10%.** This is lower than the number reported by librarians, potentially as CISOs have less direct contact with students.

There was also a shared understanding that, while use of these sites is discouraged, students can access them on their personal devices. In well-funded institutions, students typically have access to necessary resources through the library, reducing the need to turn to pirate sites. That said, one CISO in the UK noted that some students were likely to use illegal websites due to their convenience and limited security awareness. They had investigated this issue internally a few years ago. **In Africa, a lack of funding could also be a cause – one CISO from Ethiopia, reported staff using Sci-Hub to access journals that the university does not subscribe to.**

"Not only in our universities, throughout Ethiopian universities, most of the staff try to access Sci-Hub in order to access different journals which request a subscription."

ICT Director, Ethiopia

"So, there is actually no need at all for them to access it through Sci-Hub. They're already licensed as a member of the university to access those things. And the feedback that we got was that Sci-Hub's just really easy to use, and using other legitimate sources is more complex, more difficult."

CISO, UK university

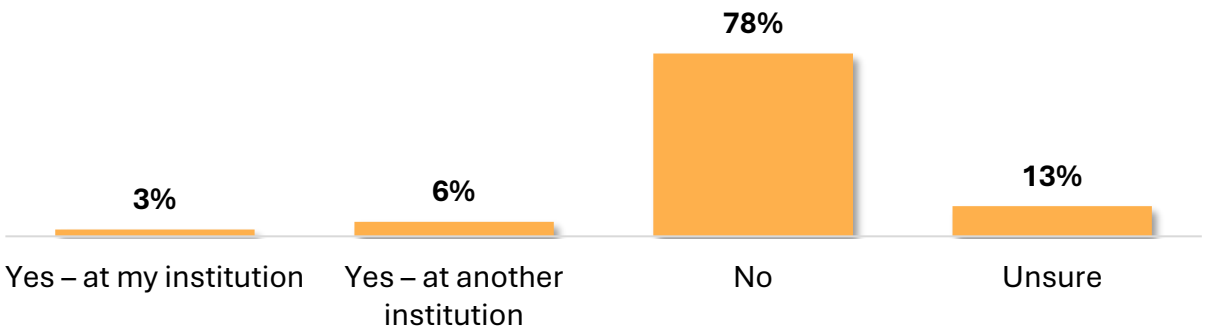
Base n = 71.

Librarians and CISOs were generally not aware of any security breaches caused by users accessing Sci-Hub

The majority of CISOs were not aware of any serious security breaches linked to the use of Sci-Hub by staff and students, at their institution or elsewhere, which compromised sensitive data or IT systems. However, **several were aware of Sci-Hub activity and reported cases of harvesting of intellectual property**. One participant, who works across multiple institutions, reported receiving alerts about several cases where Sci-Hub was harvesting journal articles using institutional credentials. Another mentioned indirect breaches involving compromised IDs, which they suspected may have originated from the use of Sci-Hub or similar platforms.

Librarians' awareness echoed this – only **3% indicated they were aware of security breaches at their own institutions related to people using Sci-Hub, while 6% reported knowledge of breaches occurring at other institutions**. These findings suggest that, while breaches related to Sci-Hub do occur, they are not widely recognised in the sector as a serious security threat on the scale of malware or ransomware.

Librarians: Are you aware of any security breaches due to people using Sci-Hub or other sites offering pirated scholarly content?



"We do sometimes get reports from publishers of potential account compromise where lots of resources have been accessed in a short space of time. And we do have quite a robust process for investigating those reports...
And we work with the library to respond to those reports as quickly as we can."

CISO, UK university

Base n = 241.

CISOs were clear that students should not use pirate sites and raised concerns about research integrity

Attitudes

CISOs noted that **most institutions strongly discourage the use of pirated scholarly content platforms**. These platforms potentially pose a direct cybersecurity threat – however, most rated Sci-Hub as a low-risk cybersecurity threat. Concerns were raised around the link between accessing pirate platforms and academic and research integrity. There was a shared belief that students and staff should not need to rely on such platforms, and that institutions have a responsibility to provide legal, reliable access to scholarly resources.

Ranking

Most interview participants rated Sci-Hub as a low-risk concern in comparison to more common cyber threats such as malware and phishing. CISOs typically prioritise risks based on frequency and potential system damage, and the CISOs we interviewed were not aware of incidents of breaches or attacks directly related to Sci-Hub or similar platforms. However, there was some recognition that these sites could still pose risks, particularly regarding the misuse or theft of user credentials.

Policy

There was a mixed picture around policies to block Sci-Hub, with notable regional differences. CISOs in the USA and Australia did not have specific policies to block Sci-Hub and were unaware of national legislation restricting access. However, some institutions have included sites such as these under broader security policies targeting potentially illegal or harmful websites. Some regions relied on blocks put in place by internet service providers.*

* Although these sites are freely accessible in many countries, others – including the UK, China, Italy and the Netherlands – have ordered internet service providers to block access.

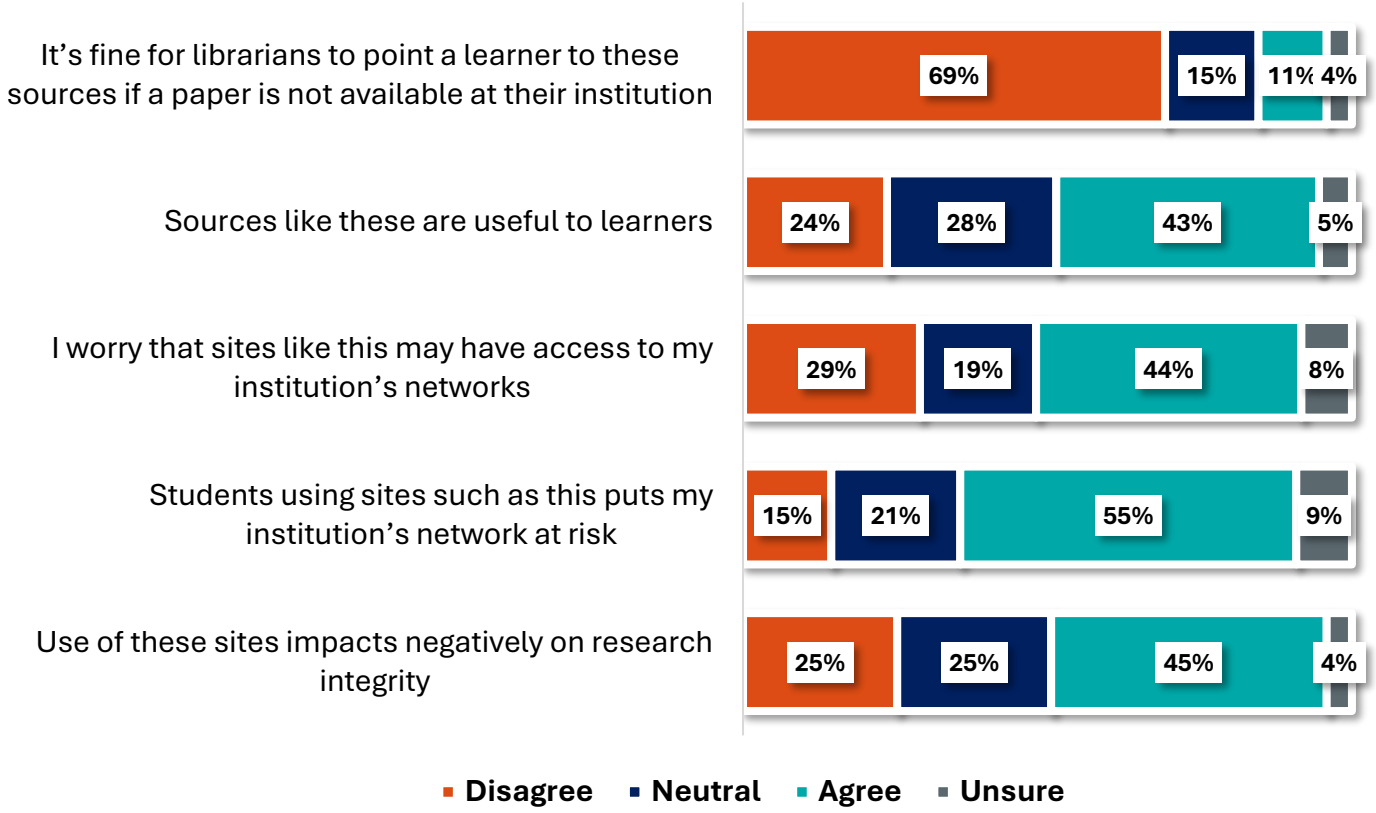
Sci-Hub's activities were considered a low-risk to overall network security by CISOs

'I would put them low. I mean, they're typically not disruptive or causing a financial impact to us. They cost us time and money, but not like website vandalism or something like that which is more visible and more painful. So [Sci-Hub] it's a nuisance crime that, you know, be nice if they stop bothering me, but it's not a huge priority.'

CISO, Large State University, USA

Librarians viewed Sci-Hub as a risk to institutional networks, but recognised its value as a resource for learners

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



Base n = 241.

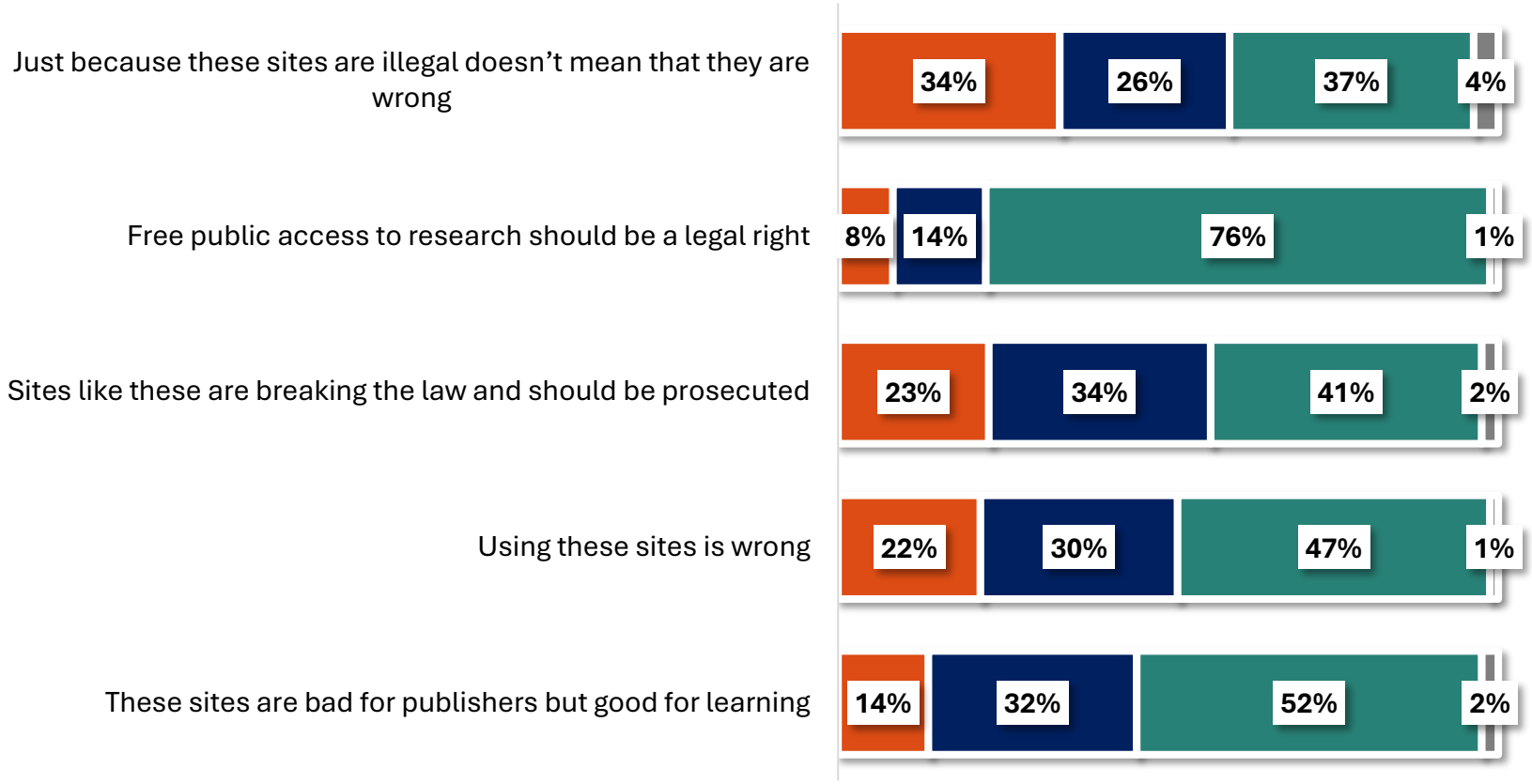
Many librarians felt sites like Sci-Hub are beneficial for learners (43%). However, this is balanced with a similar proportion who were concerned that these sites pose risks to institutional networks and research integrity (45%), a new perspective explored in 2025.

Overall, attitudes remain consistent with 2021, but there were some key differences, including:

- An increase in the number of librarians who thought that using pirate sites would put their institution at further risk (55% vs 45% in 2021.)
- Librarians in Africa were significantly more likely than those in other regions to believe it was acceptable to direct learners to sites such as Sci-Hub. This may be because access to academic resources here is more limited than in other regions.

Librarian Attitudes to Sci-Hub

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



Base n = 241.

Disagree **Neutral** **Agree** **Unsure**

Librarians' attitudes remain similar to 2021. Most librarians thought that public access to research should be free (76%). While many librarians agree that using these sites is wrong (47%) and that they break the law (41%), they also tended to support some of the underlying principles that sites like these claim to provide.

Interestingly, there was an increase in the number of librarians who disagreed that these sites are breaking the law and should be prosecuted (23% vs 13% in 2021).

Librarians called for greater collaboration and knowledge sharing between IT security staff and librarians

Librarians felt greater collaboration and better education for students/other library users and librarians were the main ways they could better work with IT and data security professionals to reduce cybersecurity risks (32%).

How do you think university IT and data security professionals and librarians can better work together to reduce cybersecurity risks, if at all? Coded open question, most common answers shown:

Collaboration between librarians and IT security staff to understand risks and concerns 32%

Educating students/users on cybersecurity risks 21%

Educating librarians on cybersecurity risks 18%

Sharing knowledge and resources, including events and webinars 12%

Additionally, some librarians recommended educating IT departments on library operations and ensuring they communicate with the library when cybersecurity issues and breaches arise (18%). A small number (5%) would consider introducing MFA for library resources, while 4% called for stricter regulation of IT usage and adherence to guidelines for users.

Q13 base n = 284, Q14 base n = 139 (2025), 172 (2021).

Similarly, CISOs recommended greater collaboration between their teams and librarians

CISOs saw cybersecurity as a shared responsibility and suggested ways in which their teams and librarians can better work together to reduce risks. These strategies are broadly grouped into the following themes:

Operational collaboration and risk management

- Coordinating on practical security measures such as risk assessments, incident response and incident recovery procedures to protect library systems and data.

Collaboration and communication structures

- Establishing formal and informal mechanisms for CISOs and librarians to communicate and share information. These included joint committees, regular meetings and sector-wide events, including external initiatives such as Higher Education Technology Agenda (THETA) in Australia and similar sector networks.

Education, training and awareness

- Enhancing cybersecurity knowledge and awareness among librarians through targeted education and practical training such as phishing simulations was seen as key.

Shared responsibility and drawing on mutual strengths

- CISOs recognised librarians' strengths as data professionals. They felt this was a good foundation for understanding and promoting cybersecurity awareness university-wide.

Policy development and compliance

- They felt librarians should be included in the development and implementation of university-wide policies and compliance measures to safeguard institutional data and systems.
- Ensuring access restrictions to library data are tested on a regular basis.

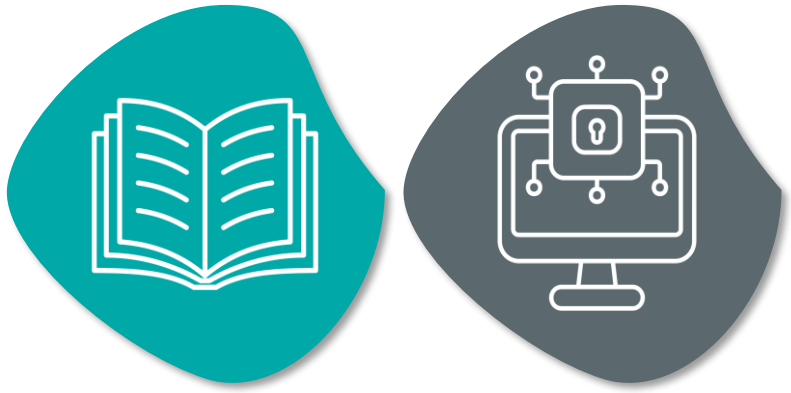
You know, these [librarians] are data science people at this point. So they tend to be pretty informed users of technology. And that tends to be a good foundation for cybersecurity awareness.

CISO, State University, USA

Conclusions and recommendations

Conclusions

- **The threat of cyber security remains high in the university sector.** 85% of librarians agreed that cybersecurity threats were on the rise for universities due to the data they hold, and their vulnerability caused by outdated systems.
- **CISOs felt they were now better equipped to protect the network** – including detecting and acting on breaches – than they were 3 years ago. MFA and other detection and protection measures have been widely adopted.
- **Piracy sites such as Sci-Hub were regarded as a 'nuisance'** compared to malicious cyber attacks such as ransomware, which threaten institutions' networks and have serious reputational and financial consequences.



Librarians and CISOs acknowledged there is a threat to academic integrity due to:

- Users interacting with AI LLM and uploading content to AI, including university IP material.
- Theft of IP by piracy sites harvesting journal articles and sharing these illegally. 55% of librarians agreed that piracy sites put their institution's network at risk, and 45% believe they negatively impact research integrity.

About Shift Insight

Shift is a global-minded market research agency that believes in the power of insight to make things better. We are proud to help clients in three key areas understand their unique and diverse stakeholders – supporting strategic decisions with robust evidence.

SHIFT LEARNING

Providing those working in education with the evidence and insight they need to make key decisions.

SHIFT MEMBERSHIP

Helping membership bodies and scholarly societies understand and support their stakeholders.

SHIFT SUSTAINABILITY

Giving organisations the evidence they need to make successful decisions that don't cost the earth.

Contact: Caroline Wheeler, Associate Director
T: 0207 253 8959
@: caroline.wheerler@shift-insight.co.uk
W: www.shift-insight.co.uk