SHIFT INSIGHT

SNSI CISOs | Research report

Caroline Wheeler and Lottie Gimlette

WWW.SHIFT-LEARNING.CO.UK

SHIFT INSIGHT SHIFT LEARNING

Table of contents

Section 1: Executive summary	3
Section 2: Background and methodology	5
Section 3: Concerns around cybercrime and data security	8
Section 4: Security breaches and mitigating risk	13
Section 5: Sci-Hub	20
Section 6: Conclusions and recommendations	29

Executive summary

This report outlines the results of online depth interviews with 11 university CISOs or ISOs based in the UK, the US, Europe and Australia. 45-minute interviews were conducted over Microsoft Teams between June and September 2022.

Main concerns

Top concerns around cybersecurity and data security centre around human error and poor cyber-hygiene practices, which result in security breaches. These are often caused by users being targeted by phishing scams, or inadvertently introducing malware onto the network via unsanctioned third-party software or hardware.

More serious concerns include ransomware attacks by organised gangs, which have been known to cause serious business disruption and considerable cost to an institution's reputation and finances.

Understanding

Respondents reported that students and staff (including faculty) have some understanding of cybercrime and data-security issues, and are concerned about privacy.

CISOs highlighted the need for cyber- and data security awareness training, but this is not always mandatory or taken up by users.

Librarians were generally regarded as having a decent understanding of cyber-hygiene/precautions, and typically comply with policies around data handling, use of encryption, etc.

Security breaches and mitigating risk

The volume of cyberattacks in the university sector was perceived as high, compared to other sectors. Whilst the level of threat remains high, security measures to mitigate these risks have improved in the last few years, to keep pace with the level of threat. One CISO likened it to an 'arms race' to keep ahead of the 'bad actors'.

CISOs had first-hand experience and knowledge of serious breaches at their own or neighbouring institutions, and were clear about the best steps to take to prevent further attacks, starting with multi-factor authentication.

Executive summary

Sci-Hub:

CISOs were aware of sites that offer pirated or illegal access to scholarly resources, but few mentioned Sci-Hub by name unprompted.

In the UK and EU, Sci-Hub was regarded as a site largely operating outside of GDPR regions.

CISOs were generally not aware of Sci-Hub being accessed at their institution, or the level of its use. They did concede that users can still find ways to access Sci-Hub, using workarounds like VPN, even if it is blocked by the institution or by national legislation.

Sci-Hub and cybersecurity:

Sci-Hub's operational model was seen as fairly low risk to an institution's immediate network security.

CISOs were highly aware of a wide range of cybersecurity threats, and those who had come across Sci-Hub (or similar sites) understood that they operate by obtaining student credentials.

They did not necessarily see a link between Sci-Hub activity and specific security breaches such as malware or ransomware attacks. This is because the file type (PDFs) that Sci-Hub uses were seen by some to present a very low risk of introducing malware onto a user's computer.

Shared or stolen credentials can be used to infiltrate and attack an institution's network (by skilled cybercriminals), however in our small sample we did not find any evidence from CISOs linking such attacks to Sci-Hub.

BACKGROUND AND METHODOLOGY

Background and methodology

Background

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, and others involved in scholarly communications.

In 2021, SNSI commissioned a survey to investigate the extent to which academic librarians were concerned about cybercrime, data security and related issues. There was a total of 278 responses, and respondents discussed themes around what they believed to be the main issues, how concerned they were about Sci-Hub, whether they saw the issue of Sci-Hub and cybersecurity as linked or separate, where they would turn to for support and their views on SNSI.

This research was commissioned by SNSI to further investigate these themes with an audience of IT security specialists working in the university sector. In this qualitative phase, we conducted depth interviews with Chief Information Security Officers (CISOs), Information Security Officers (ISOs) and senior IT staff such as Chief Information Officers (CIOs) or those in senior advisory roles in IT services organisations.

Methodology

- Online depth interviews were conducted with 11 CISOs/ISOs in the UK, the US, Europe and Australia.
- 45-minute interviews were conducted over Microsoft Teams.
- This qualitative research represents the views of a small sample of CISOs (and related roles), and cannot be extrapolated to represent the sector as a whole.

Profile of respondents

	Location				
Job roles	**UK**	**EU**	**US**	**AUS**	**Total**
CISO	2	1	1	-	4
ISO	1	1	1	-	3
Senior CISO/CIO/ advisory role	1	-	2	1	4
Total by region	4	2	4	1	11

Research objectives

Research objectives:

- Seek to understand their main concerns in relation to cybercrime, data security and related issues
- Uncover what they feel the main issues are, e.g. the main themes they are investing in to improve security at their institution
- The extent to which they are aware of and concerned by Sci-Hub
- The extent to which they see these two issues (cybersecurity and Sci-Hub) as linked or separate
- Are they aware of SNSI?
- What are their views on SNSI?

Topics discussed in the interview included:

- Their main concerns in relation to cybercrime, data security and related issues
- How well these risks are understood by faculty, students and librarians
- Specific concerns around research data and libraries
- Examples of security breaches and mitigating risk
- Awareness of Sci-Hub and access to Sci-Hub at their institution
- Risks associated with Sci-Hub
- Awareness of SNSI and any recommendations

CONCERNS AROUND CYBERCRIME AND DATA SECURITY

Over half of university CISOs interviewed rated the level of cybersecurity risk in the university sector as 7.5 out of 10 or above

Respondents were asked how worried they were about the level of cybersecurity risk within university sector in general, with 1 being low risk and 10 being high risk. Answers varied from 6-10, with over half rating the concern at 7.5 or above. There were multiple reasons why respondents believed universities a high-risk sector, including:

- The conflict between Ukraine and Russia.
- The distributed nature of research and university institutions, compared to traditional corporations and governments, making it difficult to put policies and security systems in place.
- The sector previously didn't appreciate it could be a target, due to its non-profit orientation and not historically investing in protecting its position.
- It was an early adopter of the internet and previous practices are no longer compatible and need to be improved.

CISOs and ISOs perceived the number of attacks on research institutions to have **increased**, as intellectual property is highly valuable. The attacks on research institutions mentioned included nation states carrying out attacks to obtain unpublished research data, particularly on COVID-19 research and viral and genetic research. Student records and medical records were also seen to be at risk.

However, some challenged the level of the threat to university relative to other sectors:

- Some believed it was relative to other sectors such as financial institutions, as education sits outside of the crypto currency trade so it's relatively outside of the main threat.
- In terms of ransom, the Australian respondent felt organisations were less at risk there compared to those in the US and UK as those countries have a reputation for paying and their currency is worth more.

"I think anyway for Russia to get a leg up on people who are not allies is always the case with them, and especially more so now, given the conflict."
ISO, State University, US

"In traditional corporations and in governments, you put a policy forward, you mandate it, people fall in line. There's standards you can deploy throughout an organisation. At a higher institution, you cannot do that, so everything you do has to be very surgical and very tactical, and limited in scope."
CISO, Public Research University, US

The university and research sector was seen to have a number of specific areas of vulnerability

SHIFT INSIGHT

Human factors

- Due to a lack of awareness and understanding, individual users can be susceptible to common threats such as phishing.
- The willingness of people to click on disruptive links and their lack of understanding of the seriousness and scale of a breach.
- There was also a perception that some users were reluctant or unwilling to comply with additional security steps such as multi-factor authentication.

Autonomous third-party products

- During the pandemic, there has been an increase in applications and services.
- These products are often not under the direct control of the institution, which makes them hard to control. Some of these are unsanctioned or unwanted hardware, whilst others need vetting.
- Systems are often highly integrated, so if one is exploited, there is a high chance that all will be exploited.

Research security being low priority

- Research software has a lower quality of security than industry software. It's a highly collaborative environment and traditional security controls that corporations put in place are not as viable in universities.
- This raises concerns about the privacy and security of institutional and academic research, as well as Enterprise Resource Planning (demographic and financial data).

Research, data and IP issues

- Universities house both student data and highly valuable research-originated intellectual property.
- Research collaborations also can create difficult conditions for security, opening up vulnerabilities and creating a threat to federally funded or private partner sponsored research.
- Particular challenges were seen when working with non-GDPR states, such as China, India and the US.

"Through the pandemic most of our institutions have added different applications and services and that has added this sprawl where we need to make sure we're vetting all of that third-party, so there is a lot of focus on that."

Director of Cybersecurity, IT Services organisation, US

"Without research software you almost cannot do anything, you have to use the software to get results. Unlike in industry where certain standards, protocols are established, in academia, research software security is of very low priority which to the best of my knowledge is different to tin industry."

CISO, Research Institution, Germany

The sector is also subject to more generic risk factors, which also impact other organisations

SHIFT INSIGHT

Volume and variety of threats	Physical crime	Difficult to learn from attacks	Other common issues
• CISOs were aware of a high volume of threats, both traditional (phishing, social engineering) and masked attacks (surveillance), and this was seen as challenging. • The attacking organisations are highly organised and well-equipped, with refined business models that are constantly evolving.	• The risk of laptops getting stolen and many not having sufficient security or encryption. • Traditional security controls are less viable as universities and research institutions control only a small percentage of the devices that reside in their environment.	• Often an incident will be hard to track and trace as perpetrators are able to script their own attack. • There is also poor communication between organisations when an attack has taken place because they worry about reputation and loss.	• Reference to issues such as malware, denial of service and ransomware. • This is normally due to poor cyber-hygiene. A small security gap can lead to significant damage and disruption.

"The lack of understanding that something as small as one IT account being breached could bring the entire university to its knees."

CIO, Large University, Scotland, UK

"We've had one case where one institution had an incident that they didn't share and another institution got compromised 3 months later."

CEO, IT Services organization, Australia

Despite having security systems in place, staff and students often don't understand the importance and need for them

Staff and students
Students were considered to be fairly digitally savvy and, despite not knowing the specifics around cybersecurity, they were seen to have an understanding of technology and be concerned about privacy.

Meanwhile, staff had an idea, but were not regularly informed because there were no mandates to receive cybersecurity training at most institutions.

The pandemic has also increased awareness of cybersecurity. However:

- Training is usually focused on those with a lower level of awareness and capability.
- In general, there were plenty of systems available to keep things safe and secure, but there was doubt about whether both staff and students were aware of and understood them.
- Misconceptions exist around the purpose of cybersecurity in universities and some may see it as a hindrance.

"The biggest area of concern is user behavior because of the complexity of what happens and because people are unaware of how prevalent cybercrime is."
CISO, Russell Group University, England, UK

"The students complain that they can't just click a button and get in, and faculty are mad that they have to put their password and ID in every day."
Information Security Advisor, State Government, US

Librarians
Most respondents felt that librarians took a cautious approach towards cybersecurity and were familiar with using certain tools to protect their institution from breaches.

For example, most were thought to know to transfer via encrypted channels when sharing passwords and administrative controls.

Respondents offered recommendations as to how staff and student awareness could be increased:
- Regular training.
- Educating people on new software to remain up-to-date.
- Public service announcements – what is happening and why.
- Pop-ups/external sender header in emails to increase awareness.
- Education around cyber threats and what to do if there is an incident.

SECURITY BREACHES AND MITIGATING RISK

CISOs gave examples of specific security breaches at their own institution, or elsewhere

The CISOs and ISOs we spoke to were able to give examples of specific incidents of security breaches that had occurred either at their own institution, or one elsewhere in their region. Most hadn't had a major incident for several years (possibly due to better detection and protection), but where incidents had occurred they fell broadly into the following categories:

- Network breach causing business disruption, disabling network drives/causing data unavailability.
- Phishing attacks that hijacked emails and caused mass spam.
- Ransomware attacks.
- Theft of intellectual property.

Specific examples given included:

- Attack on a German university department that disabled the network for 36 hours.
- University California San Diego being the victims of a ransomware attack, which was disclosed in the public domain.
- A UK university example of malicious business disruption by the Lapsus$ group, which may have been financially motivated, but was stopped before any ransom demand. In this case, social engineering was used to harvest the credentials of an individual who had a permission level that allowed the attack to escalate.
- Entire PhD research being stolen and published in China.

"Yes, it was a particular focus almost at the level of social engineering to harvest credentials. One individual who happened to have a permission level that allowed the dreaded thing in IT security which is continued stepping up of permissions until it got to the point where essentially the criminal gang had complete control over the identity and passwords of all individuals at that university. It is the rolling snowball … This was very well contained but it was a major incident, and it did cost hundreds of thousands of pounds."

CIO, Large University, Scotland, UK

The level of risk in universities *has not* gone down in recent years, but security measures have improved

Most respondents we spoke to agreed that the threat of network security breaches from cybercrime activity has either increased, or at best remained the same, in the university sector in recent years. What has changed is that IT security tools for detecting and preventing attacks have improved significantly.

- One CISO described the level of threat as an 'arms race', with security measures trying to keep pace with the hackers and bad actors.
- Two US-based CISOs had seen a decline in copyright infringement traffic in recent years.
- One factor that remains constant is the sheer volume of attacks experienced in the research and university sector (see next slide).

"We've strengthened our security posture and as we've done so, the number of security incidents has reduced and as a result of that, we haven't experienced a major incident for, I wouldn't know exactly the date, but certainly not for the last 18 months, maybe a bit longer. Beyond that, we did experience incidents. On that basis, the threat is not reducing, but the manifestation of the threats is reducing."

CISO, Russell Group University, England, UK

"It is difficult to tell because the tools for monitoring and alerting we have now we didn't necessarily have two years ago. So the landscape has changed. So it is difficult to tell whether it is more or less, it is hard to tell whether it is because of better reporting or better alerting or is it because things have increased or decreased?"

ISO, Russell Group University, England, UK

In their own words | Volume of attacks in the university sector

"Again, this is under threat intelligence, what I didn't mention is the sheer volume of attacks on the HE sector is an order of magnitude greater than any other sector on the planet. This is evidence from a number of sources including the national and international Microsoft networks who do a lot of our threat protection and intelligence as well. It's the sheer volume. You can break it down to all of the component parts, but it is every single type of attack from cheap and nasty phishing campaigns right down to masked attacks, we've even had fileless attacks which are very sophisticated which were directed by some particularly well skilled actors infiltrating one of our organisations relatively recently, this year. The standard threats apply but on a much larger scale.

There are a number of reasons for that, one being that higher education is seen as a soft target which is well resourced in terms of not only information but also in terms of available monetisation. You've got thousands of people working there, you've got grants going through, you've got a whole manner of things that can be extorted, stolen, or taken through. You've got a huge attack surface for the university because a lot of our members operate internationally. They also work in partnership with literally thousands of support, research institutions, organisations, you'll know this very well yourself. A lot of this information research is highly lucrative, highly sensitive, it has to be deeply protected. There is a huge target on this sector's back, and threat actors and malicious individuals are thieves by any other name, and this is something juicy that they've got their hands on, it's going to attract them."

CISO, Group of Universities, Scotland, UK

The library wasn't seen as a specific area of weakness for cybersecurity compared to other parts of the institution

Assuming the library had up-to-date security measures (cyber essentials) in place, it was seen as no more likely to be the source of a cyberattack than any other parts of the institution.

"You're not going to get access to the HR or finance systems from a library but the risk, and it's relatively easy to contain that. Just do your proper hygiene of the library, make sure it's safe, make sure it's secure … and make sure people can't see stuff they shouldn't."

CISO, Group of Universities, Scotland, UK

That said, CISOs were aware that applications accessed in public, or through a public kiosk computer, were more at risk of having malware attached to them suspiciously.

Library IT vs central IT services

CISOs identified a lack of collaboration between the central university, IT security and library IT services as a potential weak link in the fight against cyberattacks and IP theft:

- Libraries often have their own IT services.
- There is sometimes a disconnect between the library and central IT services, including centralised IT security.

"In institutions that are not collaborating with the librarians with their IT and, more appropriately, their IT security people, [it] is a risk. I think having good communications and good collaboration helps everybody. So when we think about risk that is important that we're working together on this."

Director of Cybersecurity, IT Services organisation, US

"Security on a device works best when it is owned and managed by a sophisticated organisation. However, the majority of students work from personally owned devices that may be poorly managed … Many tend to use the same usernames and passwords in the library as they might do for critical systems, and they might flick between personal use and library services. If someone acquired a student's login details they could generate phishing activity from a credible source, or it could be used to act as a 'staging point' for ongoing activity once access has been achieved, from viruses to ransomware."

Information Security Advisor, State Government, US

CISOs were aware of IP theft arising from the library, but it was not their number one concern in the fight against cybercrime

The CISOs we spoke to were aware of the threat of attacks on intellectual property, including library journals, unpublished research or other scholarly material that sits behind a paywall, and the use of university credentials to facilitate that theft. Some CISOs were able to give examples of such attacks, including one at their own institution:

- One CISO gave an example of *"an Iranian group who have exfiltrated substantial volumes of scholar material and made them available on the dark web or other such type surfaces."*
  CISO, Russell Group University, England, UK
- Another described past incidents of library IDs being compromised and used to exfiltrate journal articles.

"[Previously] the library did not use federated authentication, meaning library users would not use their university credentials to access resources, they would get a library patron number and set a pin, and from my time working in the library, we had multiple instances where these ID and pin numbers were compromised and used to exfiltrate tons of scholarly journal articles and other unauthorised database access, so while it's not theft of any of our own data, we're being used as a conduit for that."
ISO, State University, US

CISOs' primary concern is the theft of personal data, including student educational records, and Enterprise Resource Planning (EPR) data, which might include HR records and financials. Intellectual property, accessed via the library and owned by a third party, was a ***secondary concern*** in the fight against cybercrime.

"We are most concerned about student data and then researching intellectual property theft second to that."
CISO, Public Research University, US

"There is also a completely spoofed network which claimed to be a research network which was being used and was sharing scholarly articles and got quite a bit of traction, but it wasn't owned by any university."
CISO, Group of Universities, Scotland, UK

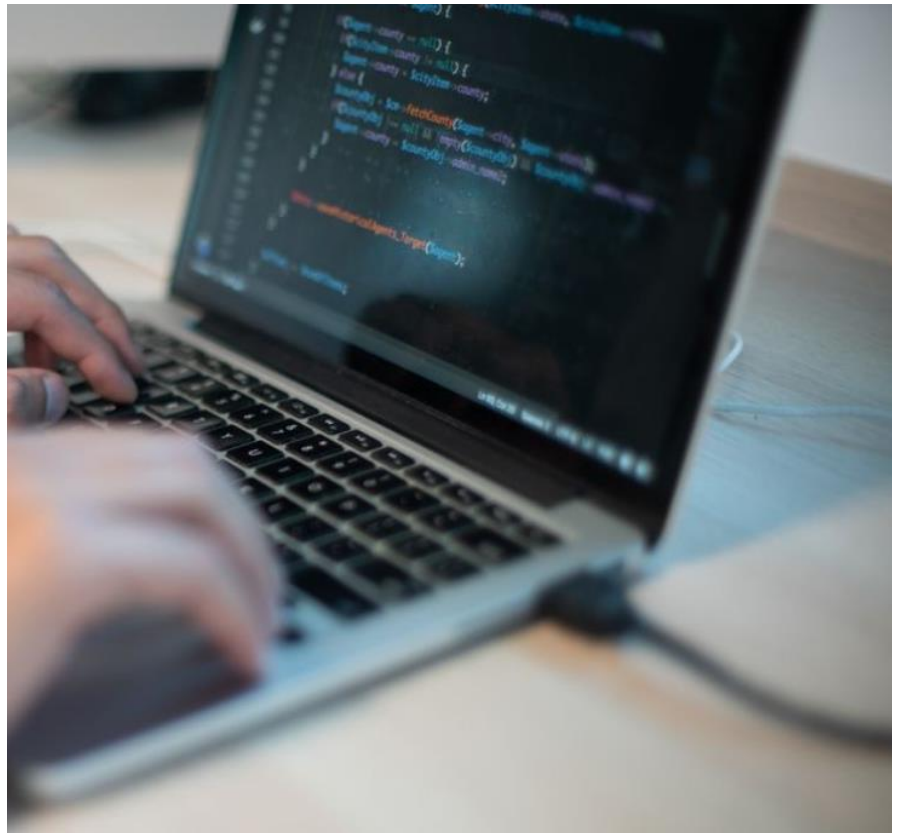
There is a *potential* risk for student or staff credentials to be used to cause a security breach, in the hands of skilled cyber attackers

In the event of a student account being compromised, IT security would do a cyber risk assessment to understand the levels of vulnerability, and establish the risk of further harm. Potential areas of concern include:

- Credentials, in the hands of skilled cybercriminals (bad actors), could be used to generate spoofing and phishing activity from a credible source, which might be used to reap credentials from or compromise university staff, students and stakeholders more widely.
- The level of access to privileged areas of the university network that can be enabled depends on the level of permissions that the account has. For example, research students may have a significantly higher level and range of access compared to standard undergraduate accounts.
- Threat actors can elevate the permissions given to an account using a number of means, including generation of security authentication tokens and administration privileges for accessible digital areas within and associated with that account.
- One CISO gave an example of the malicious group Lapsus$ using this method of attack:

  "In other words, all and any systems, applications available to the compromised account would be vulnerable to secondary attack by means of hijacking and escalation techniques."

CISO, Group of Universities, Scotland, UK



SCI-HUB

University CISOs were aware of websites that offer pirated or illegal access to scholarly resources, but most did not mention Sci-Hub unprompted

Awareness of Sci-Hub

- Of the 11 respondents we spoke to, only 2 mentioned Sci-Hub by name unprompted, when we asked if they were familiar with any websites that offer pirated or illegal access to scholarly resources.
- One CISO who was familiar with Sci-Hub also mentioned Library Genesis in relation to content piracy.
- Other CISOs were aware of such sites, and one referred to a site hosted in Russia that contains 'a lot of scholarly research, highly distributed', but did not mention Sci-Hub by name.

Prompted awareness

- When prompted, all but 2 respondents had come across Sci-Hub in their professional capacity.
- Those CISOs working in a more senior/strategic role in their organisations were most familiar with Sci-Hub's activities.
- One US respondent was able to give an example of an incident several years ago where journal articles were exfiltrated from his institution's library, and Sci-Hub was suspected to be the end destination.
- One UK CISO could not recall being alerted about Sci-Hub specifically by name, but could recall a notification about a similar site.

"There's a tonne of it available. Starting with the old pirate bay back in the day, which I think it's down now, there's several in Russia that are hosted in Russia that contain a lot of scholarly research, highly distributed. There's some in Brazil. I don't think I could name them. There's a lot of them out there."

CISO, Public Research University, US

"Yes, we are, and they are outside of GDPR. Within Europe, it's very rare, but there are open research sites pretty much all over the globe. India is very keen on this. So, yes, I am, can we do anything about it? No. That is the short version."

CISO, Group of Universities, Scotland, UK

"We know about Sci-Hub, and we know about the potential for universities in other continents potentially using Sci-Hub and the like for access."

CIO, Large University, Scotland, UK

University CISOs were generally not aware of Sci-Hub use by students or faculty, or the extent to which it might be used at their institution

SHIFT INSIGHT

Access to Sci-Hub

Respondents in this research were not aware of students or researchers at their institution accessing Sci-Hub, for a number of reasons:

- Perceived need: students and researchers in the UK, the US, EU and Australia have good access to subscription journals via their institution, and therefore less of a need to seek out Sci-Hub.
- Lack of visibility: CISOs in the US see Bit Torrent traffic, but do not have visibility of what students are downloading.
- CISOs are not close to academic activities. One UK CISO noted that librarians may have more awareness of Sci-Hub use.

However…

The culture of openness in research and universities did create the possibility, for some, that users may seek to obtain educational material for free by finding ways to bypass paywalls.

"Do they use Bit Torrent as a protocol, yes? Do we have visibility into what they're downloading, no, because in the US students have an expectation of privacy at the university, so we cannot inspect the type of traffic that is associated with our students. It's very likely. We do see Bit Torrent traffic quite a bit, but as to what in particular, I could not speak to that."

CISO, Public Research University, US

Access to Sci-Hub in regions where it is blocked

CISOs in the UK and EU, where Sci-Hub is blocked, were typically unaware of the extent to which students and researchers were still accessing Sci-Hub. They were aware that *it is still possible* for users to do so, from outside of the university network.

- IT security can prevent access on devices managed by the institution, but not personal devices.
- Sci-Hub can be accessed using workarounds such as VPN:

"If they want to, they will find working URLs."

CISO, university Institution, Germany

"Clearly that doesn't prevent people from accessing it from outside of our network, but we also have controls in place on all devices that we manage to deal with that sort of issue. Again, that doesn't address that concern for devices that are personal devices."

CISO, Russell Group University, England, UK

Sci-Hub was often regarded as lower risk because of file format

For CISOs, Sci-Hub was regarded as a lower risk of introducing malware that could cause a network breach. The main reason given for their lack of concern was that the file type used by Sci-Hub (PDFs) was not one typically associated with malware. Sci-Hub was therefore seen to present a lower risk than other illegal file-sharing sites accessed by users, for example, to download music, videos or apps.

Despite this relaxed view of the dangers of Sci-Hub, one respondent did indicate concerns:

- Sci-Hub encourages credentials sharing – which in itself is a breach of the terms of their institution's privacy policy.
- There was an implicit danger associated with Sci-Hub due to it being well known (in this case). This respondent feared that increasing publicity and visibility might mean that people would become more likely to try and access it.

"By rating it as a 2 I am not diminishing the potential, but in my experience, I am not seeing it."

CIO, Large University, Scotland, UK

"Bit Torrent is a tiny percentage of all the traffic, and the purpose of Sci-Hub, the file type it typically shares is not commonly associated with malware or things like that … Compared to one of the other sites where individuals are downloading music, videos and applications, there's a much higher percentage of potential malware infections from that than Sci-Hub."

CISO, Public Research University, US

"Should someone access Sci-Hub, download a load of malware onto their machine and as a result of that connect to our network and their machine be detected and identified as hosting malware, we would quarantine that machine and then require it to be cleaned up before it could function on the network. We wouldn't know where that malware had originated."

CISO, Russell Group University, England, UK

The threat to network security posed by Sci-Hub, and the threat to research and the academic record, were seen as separate, but *potentially* linked

Whilst CISOs typically ranked Sci-Hub as a lower threat than other illegal file-sharing websites, in terms of cybersecurity and network breaches, they did acknowledge the threat to the scholarly record, and the potential for sensitive research to be shared with politically motivated organisations and nation states.

As mentioned earlier, CISOs were aware of the theft of intellectual property, including unpublished research data ending up in the hands of nation states. In our small sample, respondents did not make a *direct* link between these thefts and Sci-Hub (as the actor).

One respondent in a senior role did raise concerns about the underlying threat from Sci-Hub being related to its origins and the potential for it to act for the benefit of the nation state of Russia.

"100% there is, there's credential sharing and they grab those from the academics … but I'm also aware of where Sci-Hub is domiciled and who is behind Sci-Hub, so it gets back to that nation state and that is where it is really difficult. For me, it is a really clear chain of evidence. If you don't think Sci-Hub is supporter owned and the outcome has been used for the benefit of Russia, then you've got to at least have a very big concern that you don't have an understanding. Sci-Hub, if we did a third-party risk assessment, we would not pass the risk assessment. We would not sign a service for Sci-Hub, there is no way you'd sign that agreement up. 100% there is the underlying threat where Sci-Hub is either domiciled or where it is supported."

CEO, IT Services organisation, Australia

The main areas CISOs were investing in to improve security at their institution included multi-factor authentication for staff and students

CISOs considered basic cyber-hygiene tools, such as multi-factor authentication (MFA), to be a key line of defence in preventing cybercriminals from accessing their university network. The main areas of security they recommended for institutions to invest in, if they weren't doing so already, were:

- Multi-factor authentication.
- Upgrading network security tools, including patching, firewalls, etc.
- Test vulnerability detection procedures.
- Cyber essentials training or certification.
- End-to-end encryption of content.
- End-point detection and response or EDR.
- Zero trust architecture or ZTA (mentioned by one senior CISO).

"So really the basic cyber-hygiene things, we really consider multi-factor authentication is huge. So in the umbrella of identity in access management, really knowing who is accessing your network."

Director of Cybersecurity, IT Services organisation, US

Additionally…

- Threat intelligence and threat sharing between institutions, and via collaboration with partners in the sector, including Our Net in Australia, JISC in the UK, Internet 2 in the US and Canary in Canada, were recommended.
- Remote working and study has impacted IT security teams' ability to police activity outside of the institution's network – particularly in relation to personal devise use, which in turn strengthens the need for MFA and increased cyber essentials training.

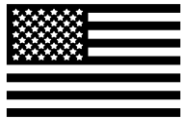
But human behaviour still presents a risk…

"I think it's going to be a work in progress. We can enable MFA for everyone, every faculty, every student, every staff until the cows come home, but if they are willing to divulge sensitive information via email or phone, it's not going to matter if somebody gets into their account if they are still willing to give up that information in some other way. It's only going to increase, so diligence is key."

ISO, State University, US

CISOs believe blocking access to Sci-Hub is a short-term fix, with mixed view on effectiveness

CISOs in the US and Australia presented a very different picture of the institutional and national policy for blocking Sci-Hub to that seen in the UK/EU. Individual CISOs in the US were broadly supportive of the idea of blocking Sci-Hub, but were aware that it was not supported by current legislation and might be seen in the academic community as infringing on someone's ability to conduct research.



US institutions would only consider blocking Sci-Hub if it presented a significant risk to cybersecurity. In general, US institutions were said to block very little, and only known malicious sites, or those coming from a threat intelligence feed. Examples included:

- C2 traffic (linked to malware).
- Crypto miner traffic or Crypto miner tools.
- Sites used for phishing where credentials are collected.

In Australia, where some institutions do block Sci-Hub, our respondent described it as a 'whack a mole' approach, due to Sci-Hub's frequent change of IP address

"When you block them they change IP address and then you end up with 1,000 blocks for Sci-Hub and the IT team are getting frustrated because it's an inappropriate use of their time with this whack a mole approach, and has diminishing returns, and it isn't addressing the underlying problem which is how we can get that solution, multi-factor authentication."

CEO, IT Services organisation, Australia

In the UK and EU, where institutions do have policies to block Sci-Hub, CISOs felt they were doing as much as they could, using their existing resources and network security tools to limit Sci-Hub and similar illegal activities. Some drew a comparison with cheating sites, which although undesirable did not cause serious issues resulting in business disruption. They described steps taken to prevent these services from promoting their offer to students.

The City of London Police warning issued to UK universities in 2021 around security risks associated with using Sci-Hub meant awareness was understandably higher in the UK and EU. One UK CISO had responded to the warning by strengthening their institution's firewalls and network security, and blocking Sci-Hub. In the US, a different picture emerged.

"In fact, that's something that would be difficult to enforce here in the United States, so while we've talked to our staff and faculty about the dangers of Bit Torrent and file sharing sites, that's not something we can prevent them from doing."

CISO, Public Research University, US

Senior CISOs recommended 2 lines of defence to limit the activities of Sci-Hub and other organisations that threaten the academic record

Multi-factor authentication

- Multi-factor authentication could be applied to journals at the point of access, making it harder for Sci-Hub to access library systems even with stolen or acquired credentials.

"If it [MFA] is not there already, it's imminent. It will be there for staff, that is a given. If it isn't there for students at the moment, it is imminent, that is the next element that needs to be applied when you're logging into a journal solution – the multi-factor, because that then shuts down, raises that bar a level higher for the Sci-Hubs of the world and makes it a lot harder."

Director of Cybersecurity, IT Services organisation, Australia

Geo-blocking

- Concerns linked to nation-state activity could be tackled through increased vigilance and geo-blocking of activity from countries such as India, North Korea, Russia and China.

"It is much more about being aware that this is going on and monitoring the activity, making sure that your political locks and blocks are in place so if anybody is operating from India, North Korea, Russia, China, you know about it and you're saying you're not getting to use our facilities. Geo-blocking is a very simple straightforward way of addressing this. It's also a good way of stopping the Nigerian prince scams. An awful lot of the non-GDPR activity can be easily closed and you can open up legitimate portals for research. That kind of knocks it on the head, unless people are going to do emitted exfiltration, in which case there is nothing you can do about that anyway."

CISO, Group of Universities, Scotland, UK

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Human error is still one of the main threats to IT security

Human error and lack of awareness around cybersecurity were concerns for CISOs, and a main cause of data security incidents

- Individuals are susceptible to phishing attacks, and may be unaware of the seriousness and scale of disruption caused, particularly if it escalates within the network.
- CISOs emphasised the importance of good cyber-hygiene, such as multi-factor authentication, reinforced with regular cybersecurity training.

CISOs' primary concern was protecting the network

CISOs' primary concern was protecting the institution's network from serious security breaches that cause prolonged business disruption and data unavailability, including ransomware attacks that attempt to monetise the disruption. They were also concerned about the protection of personal data, including HR, medical and financial information.

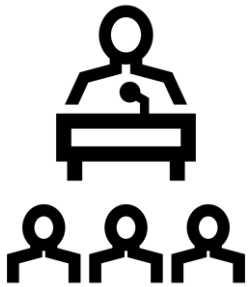
- CISOs were less concerned about staff and students accessing and downloading copyrighted material from illegal or pirate websites, because the file types concerned (typically PDFs) present a very low risk of introducing malware into the network.
- When malware is detected by IT security, they don't necessarily know where it originated from.
- Some CISOs were aware of incidents of credential theft (or harvesting) being used to exfiltrate scholarly journal articles from their own institution or elsewhere. Our respondents did not have recent examples of this activity, and did not attribute it to a known source such as Sci-Hub.

CISOs did not make a direct link between security breaches and Sci-Hub, but it is possible…

CISOs were concerned about the threat of politically motivated cybercrime sponsored by nation states targeting sensitive research data. There have been incidents where COVID-19 research was targeted. One CISO made the link between these incidents and Sci-Hub, due to Sci-Hub being located in Russia, and hinted at the possibility of Sci-Hub being supported by the Russian state. That said, this hypothesis is not supported by direct evidence found in this research.

Recommendations

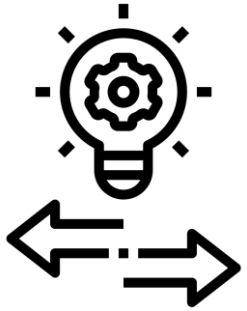
Raise awareness of SNSI amongst the IT security community



There is an opportunity to raise awareness of SNSI's mission to combat the threat of cybercrime, through closer collaboration with the IT security community in universities and research institutions by having:

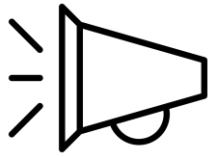
- Greater visibility at events, conferences and online communities visited by CISOs and IT security specialists working in the sector
- Thorough collaboration with organisations that already operate sector-level cybersecurity groups, such as Our Net in Australia, JISC in the UK, Internet Two in the US and Canary in Canada, in addition to the National Cyber Security Centre in the UK.

Information and intelligence sharing



- The CISOs we spoke to had low awareness of the extent to which Sci-Hub was being accessed and used at their institution.
- SNSI could help to bridge this knowledge gap, by finding and sharing data on the extent of Sci-Hub use within institutions, and publicising this to CISOs.
- In turn, this would provide an opportunity to increase understanding of how Sci-Hub operates and the potential risks to data security.
- Raising awareness of Sci-Hub in the university IT security sector in turn would potentially increase vigilance and monitoring of its activities.

Campaign to promote good cyber-hygiene practices



- SNSI could join forces with IT or librarian groups in the sector, to reinforce the importance of mandatory cyber essentials training for all students, staff and faculty members.
- Consider sponsoring training and awareness campaigns to promote the take-up of multi-factor authentication and help users understand the importance of this.

SHIFT INSIGHT LTD
THE DEPARTMENT STORE STUDIOS
19 BELLEFIELDS ROAD
BRIXTON
LONDON SW9 9UH

T: +44 (0)207 253 8959
E:

SHIFT
LEARNING

SHIFT
SUSTAINABILITY

SHIFT
MEMBERSHIP