A toolkit to support librarians

How to engage your institution's security team on cybersecurity and piracy threats and initiate and maintain meaningful conversations

SNSI

Introduction

About the toolkit

The higher education sector is particularly vulnerable to cyber-attack due to the large amount of personal and research data that universities, including library systems, routinely store.

At the 2023 Charleston Conference, SNSI hosted a debate to explore where responsibility for campus network security lay – with librarians or IT security.

We heard that:

- While campus network security is not the primary responsibility of librarians, there are pieces that the library is responsible for and therefore must be knowledgeable about.
- It is important that campus administrators understand the interactions libraries have with data and other pieces of sensitive information.
- There is an inherent tension between libraries and campus IT: IT is concerned with keeping access to information restricted while the library is concerned about granting access to information.

The overwhelming message, though, was a request from librarians for help and support in their conversations with campus network security colleagues.

This toolkit provides librarians with practical guidance on how they can help their institution's security team(s) better understand the cyber threats they are facing and their implications for the institution as a whole.

Visit www.snsi.info for more information.

Contents

- **Top Tips**: How to start a dialogue with your security team about current cybersecurity and piracy concerns.
- **Expert Insights**: Understand the unique insights and expertise that CIOs and CISOs bring to cybersecurity strategy and implementation.
- **Risk Assessment**: Learn how to request and utilise detailed risk assessments from your security department to identify vulnerabilities.
- **Collaborative Approach**: How to build a collaborative environment to develop and refine cybersecurity policies and procedures.

Top Tips

How to start a dialogue with your security team about current cybersecurity and piracy concerns

Top Tips

1. **Stay informed.** Keep up-to-date with your institution's cybersecurity policies. They often reflect the latest standards and best practices that you can adopt in the library. Ask about newsletters or alerts provided by your institution to stay abreast of updates and threats.

2. **Initiate dialogue.** Reach out to members of your campus IT and set up a meeting to discuss your library's cybersecurity concerns. Come prepared with a list of questions and ask about potential risks, recent trends in cyber threats, and how they might impact library services. Familiarize yourself with basic cybersecurity terms to communicate more effectively, and be aware of data privacy regulations (GDPR, CCPA) and how they relate to your library and university to ensure compliance.

3. **Know your concerns.** Bring up scenarios relevant to your library's operations, such as safeguarding sensitive patron data, managing backups, or providing service continuity during an outage or cyberattack. This will help your campus IT provide more targeted advice.

4. **Understand current measures**. Request a walkthrough of the current security measures in place for your institution and how they protect library resources. Inquire about identity and access management practices and data encryption policies. Take this opportunity to identify any gaps in your current practices. Are there any services that exist outside these measures that your IT department should be aware of?

Top Tips (2)

5. **Encourage collaboration.** Inquire about training sessions that library staff can attend to stay up to date on the latest security initiatives or propose working on joint projects, such as developing library-specific security and service continuity plans. Keep an eye out for future conference opportunities to share what you have learned.

6. **Engage across campus**. Are there any technology or cybersecurity committees at your institution? If so, get involved to learn about new security initiatives and technologies. Reach out to faculty members who specialize in IT or cybersecurity; they can offer insights into cybersecurity best practices and may be willing to collaborate on library-specific projects or presentations.

7. **Participate in awareness campaigns.** Partner with IT to create cybersecurity awareness materials tailored for library users. A perfect opportunity for this is during the national Cybersecurity Awareness Month, held annually in October. Take advantage of this opportunity to collaborate with your campus IT to organize workshops, create displays, or host guest speakers on topics like data privacy, safe browsing habits, and recognizing phishing attempts.

8. **Watch your network.** Keep in touch with your network administrators and keep abreast of local attacks and successful incursions – get regular updates if possible. What areas of your campus are being targeted, and where are bad actors finding success? Are there lessons to be learned in the library? What lessons are you learning that need to passed along to all library staff and users?

Expert Insights

Understand the unique insights and expertise that CIOs and CISOs bring to cybersecurity strategy and implementation

Expert Insights

1. **Security has an organizing principle.** Even if your institution doesn't have a security or compliance team, someone or even a whole team is probably practicing good security hygiene in their little corner, or some teams may have implemented security basics in response to regulatory and compliance requirements. But the best way to approach security is as an entire organization, and that requires, well, organization!

2. **Your institution's awareness of security impacts your security health.** Your institution's security depth is directly proportional to the number of people in your organization who understand security basics and practice them. This requires you to have a shared understanding of security throughout your institution – from your employees, to your executive team, to your board of directors.

3. **Your institution's culture impacts your security health.** If your institution is highly siloed, or communication across teams is poor, your path to security healthiness will be more difficult.
   A security program may highlight cultural weaknesses.

Expert Insights (2)

4. How you use technology is more important than what you use. You could spend all the money in the world on technology and tooling, but you'll never achieve security healthiness if you're not using that technology in a way that best supports your institution’s business objectives.

5. Security requires leadership to stay healthy. The executive team has to be one hundred percent committed to securing your institution for it to be successful. More importantly, they need to have meaningful insights and metrics that help them best understand how security is reducing the institution’s overall business risk, and to understand when they need to invest more into or change how they’re investing in the security program.

6. Security requires constant vigilance to stay healthy. Security isn't a “climb to the top of the mountain” activity, where you're done once you've reached the peak! Security is a “steer the ship through the rocks to keep the boat from running aground” activity. There is almost never a “set it once and done” task or technology in security.

Risk Assessment

Learn how to request and utilize detailed risk assessments from your security department to identify vulnerabilities

Risk Assessment

Risk assessments are critical for libraries, especially in academic institutions where sensitive information is handled. By identifying vulnerabilities, libraries can take proactive steps to prevent security breaches. Here are ten recommendations to help libraries assess their cybersecurity preparedness effectively:

1. **Engage with your institution's security department early.** Collaboration is key. By engaging early with your security department, you can ensure that they understand your specific needs and the sensitive data the library handles, such as research data and student records. Early involvement leads to more tailored and effective risk assessments.

2. **Identify critical digital assets.** Libraries handle a variety of resources, including digital archives, databases, and subscription services. Identifying which assets are most critical to operations helps prioritize security measures around the most valuable or vulnerable data.

Risk Assessment (2)

3. **Review and update access control policies.** Ensuring that only authorized personnel can access sensitive systems or data is a basic security measure. Regular reviews help to update who has access, minimizing the risk of insider threats or accidental breaches.

4. **Map out data flow and storage.** Understanding where data is stored, how it moves across systems, and who can access it is essential for identifying potential vulnerabilities. A well-documented data flow helps pinpoint areas where security could be weak or outdated.

5. **Perform regular vulnerability scans.** Vulnerability scans identify weak points in your digital infrastructure. By running these scans regularly, you can detect outdated software, misconfigurations, or other issues before they are exploited by attackers.

6. **Evaluate third-party vendors and tools.** Libraries often rely on third-party vendors for cloud storage, databases, or software. These external services can introduce vulnerabilities. Regularly assessing the security measures of your vendors ensures that their practices meet your institution's standards.

7. **Simulate cyberattacks (penetration testing).** Penetration testing helps simulate a cyberattack on your systems. This hands-on approach helps identify weaknesses that may not be detected by routine checks and prepares the staff for real-world scenarios.

Risk Assessment (3)

8. Assess the security of mobile and remote access. Many library services can be accessed remotely, making mobile and remote access a potential vulnerability. Ensuring that remote access is secure with tools like VPNs or two-factor authentication is crucial to prevent unauthorized access.

9. Include user behavior in risk assessments. Employees, students, and external users may inadvertently introduce security risks. Reviewing how users interact with library systems (e.g., phishing awareness, password practices) provides insight into potential human vulnerabilities.

10. Incorporate incident response capabilities. A well-prepared library is one that not only assesses risks but is ready to respond to them. Reviewing your incident response plan as part of the risk assessment ensures that, in the event of a breach, the library can respond quickly and effectively to mitigate damage.

By requesting and utilizing detailed risk assessments, libraries can create a comprehensive cybersecurity strategy that addresses both digital and human vulnerabilities.

These recommendations offer a structured approach to preparing for and managing potential cybersecurity threats within academic institutions.

Collaborative Approach

How to build a collaborative environment to develop and refine cybersecurity policies and procedures

Collaborative Approach

1. **Create a cross-functional team.** Suggest forming a working group that includes librarians, IT staff, and the cybersecurity team to regularly review and update cybersecurity policies. This ensures policies reflect both the library's unique needs and broader institutional goals.

2. **Join broader security initiatives.** Ensure alignment in protecting access to resources such as e-books, databases, and research repositories – helping to reinforce consistent application of security protocols, including two-factor authentication for accessing resources. Being part of broader institution-wide security initiatives helps your library become a valued partner in cross-departmental cybersecurity policy development.

3. **Identify and agree shared goals.** Emphasize the shared mission of protecting institutional assets. Ensure all parties understand that cybersecurity is a collective responsibility, with libraries managing digital content, access rights, and patron data.

Collaborative Approach (2)

4. **Establish regular communication.** Encourage the creation of a communication pipeline, where updates from the IT and cybersecurity teams on the latest threats or best practices are regularly disseminated to the library staff.

5. **Ensure policy iteration.** Cybersecurity policies should be living documents. Libraries should work with cybersecurity teams to continuously refine these policies based on evolving threats and emerging technologies.

6. **Arrange content provider check-in.** Initiate a discussion with your publishers and content providers to gain insight into their security policies and any concerns. Are there specific preferences regarding authorization and authentication practices that the library could proactively adopt to help minimize potential service disruptions?

Doing more: we want to hear from you

Part of SNSI's objective is to be a strong partner for our communities. As we move forward together, questions we are asking ourselves include:

- What support do librarians need from publishers and technology providers to better manage and navigate the need for access with the need for security and data protection?
- How can we work with IT security within institutions to design systems that meet both researcher and organisational goals to help people prioritize safety over convenience?
- What support do institutions need to implement and uphold a secure network system to safeguard users and ensure streamlined simple access?
- What more can publishers do to make their platforms easy to access so people don't use pirate sites?
- How can we better work together to address challenges of balancing security and simple authentication methods from multiple locations and devices?
- Is more internal education and training needed around the wider threats of cyber and data breach?

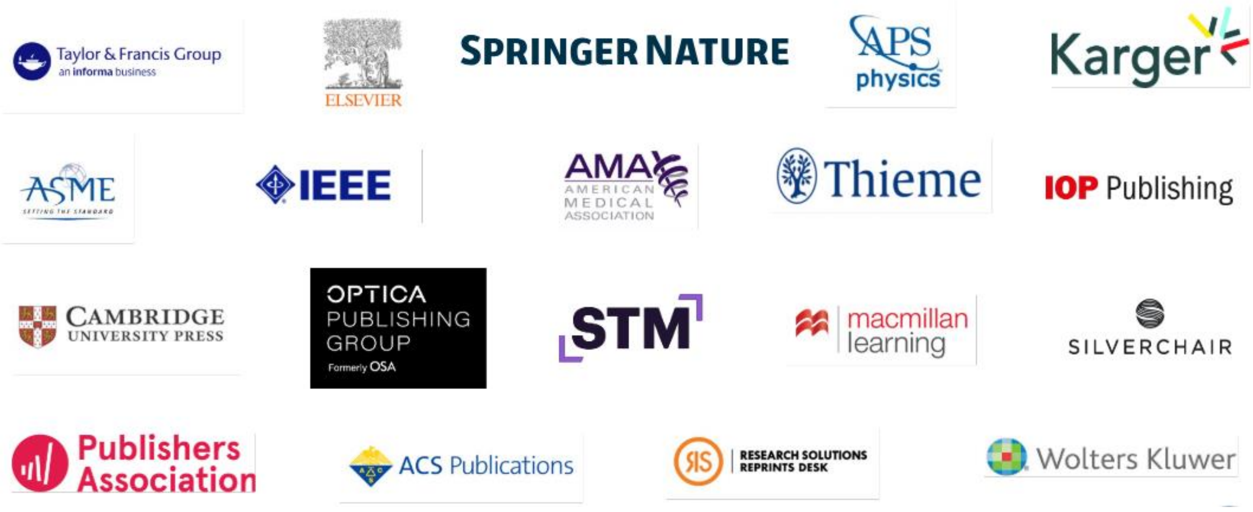
We want to hear from you!
Contact us via the website www.snsi.info

SNSI

About SNSI

- SNSI brings together publishers and institutions to solve cyber-challenges threatening the integrity of the scientific record, scholarly systems and the safety of institutional and personal data.
- Members include large and small publishers, learned societies and university presses and others involved in scholarly communications.

Participating organizations



About SNSI University Relations Group

The SNSI University Relations Group works to help raise awareness of shared vulnerabilities, discuss challenges, develop solutions and ways to improve the user experience, while providing legitimate access to scholarly content. Participants include publishers, librarians and other key industry stakeholders.

Members:

- **Gwen Evans,** VP, Global Library Relations, Research Networks at Elsevier.
- **Helen B. Josephine**, Principal, HBJ Associates.
- **Juan P. Denzer**, Engineering and Computer Science Librarian, Syracuse University Libraries.
- **Emily McElroy,** Vice President for Academic Relations, Taylor & Francis.
- **Rick Anderson**, University Librarian, Harold B. Lee Library, Brigham Young University.
- **Stacy Best Ruel**, Director of Marketing, Key Accounts, Americas Springer Nature.
- **Sharon Mattern Büttiker**, Director of Content Management, Research Solutions, Inc.

About SNSI University Relations Group (2)

Members:

- **Sari Frances**, Dir. of Content Protection Services, Elsevier (Co-Chair).
- **Scott Levi Ahlberg**, Chief Operations Officer, Research Solutions and Reprints Desk, Inc.
- **Andrew J. Wesolek**, Director, Digital Scholarship and Communications (DiSC), Jean and Alexander Heard Libraries, Vanderbilt University.
- **Jamen McGranahan**, Associate Director of Library Technology & Assessment Services, Vanderbilt Library, Vanderbilt University.
- **John Felts**, Head of Information Technology and Collections / Librarian, Coastal Carolina University.
- **Natasha Nekola**, Sales Manager US and Canada at the JAMA Network.

For more information,
please visit www.snsi.info