

Chapter 5

A Systemic Approach to Cybersecurity in International Research Projects. The Role of Digital Platforms

SŁAWOMIR WYCIŚLAK

Institute of Economics, Finance and Management

Jagiellonian University, Kraków, Poland

ORCID 0000-0002-8913-1634

Abstract: Digital platforms have become essential to international research projects. This reliance has amplified cybersecurity challenges in academic environments. A systemic approach is needed to balance open scientific practices with security requirements. This article examines cybersecurity in international research collaborations through three key components: input quality and data sources, data processing methods, and research outputs. By analyzing commonly used research platforms, it identifies critical vulnerabilities in current workflows and proposes strategies for building a robust cybersecurity culture in academic settings. These include comprehensive awareness programs, regular training sessions, shared responsibility frameworks, and academic-private sector collaboration. Digital platforms transform the research ecosystem by enhancing scientific productivity. However, they also introduce new cybersecurity challenges requiring careful mitigation. By adopting a balanced approach, the scientific community can harness digital platforms' potential while safeguarding the integrity and security of international research projects.

Keywords: Cybersecurity, international research collaboration, digital platforms, risk management, data security, academic research infrastructure, open science, cybersecurity culture

Introduction

In an era of increasingly interconnected global research, the importance of robust cybersecurity measures cannot be overstated. This article delves into the intricate landscape of cybersecurity challenges faced by international research collaborations, with a particular focus on the pivotal role of digital platforms. We explore a systemic approach to identifying and mitigating risks across the research lifecycle, from data input and processing to output management. The analysis encompasses key elements such as data integrity, access control, and provenance, while also addressing the unique challenges posed by diverse data sources and collaborative environments. Furthermore, we examine strategies for cultivating a strong cybersecurity culture in academic settings and discuss the transformative impact of digital platforms on the research ecosystem. By adopting a holistic perspective, this article aims to equip researchers and institutions with the knowledge and tools necessary to navigate the complex cybersecurity terrain of modern international research projects.

Systemic Approach to Cybersecurity Threats in Research Projects

In the context of international research collaborations (IRC), the management of inputs, processing, and outputs presents unique cybersecurity challenges. This analysis examines these key system elements, focusing on risk identification, mitigation, and control strategies within the IRC framework.

The utilization of diverse data sources as inputs in IRC introduces cybersecurity vulnerabilities. These include maintaining data integrity across multiple sources, implementing effective access control mechanisms for sensitive information, and ensuring clear data provenance for both reproducibility and security audits.¹ To address these challenges, institutions and researchers must implement robust data management practices encompassing rigorous source verification procedures, secure data transfer protocols, comprehensive metadata management systems, and regular data quality assessments.

Risk identification in this context involves recognizing potential threats to data integrity, confidentiality, and availability. These may include unautho-

¹ Joachim B. Ulven and Gaute Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," *Future Internet* 13, no. 39 (2021).

rized access, data corruption during transfer, or inconsistencies in data formatting across sources.² The complexity of these cybersecurity challenges necessitates a systemic approach to risk management in IRC projects, considering the interconnected nature of data sources, research methodologies, and collaborative networks.

Mitigation strategies should focus on implementing multi-factor authentication for data access, utilizing encryption for data transfer and storage, and developing standardized data formatting protocols across collaborating institutions.³ Control measures should include regular security audits, continuous monitoring of data access logs, and the implementation of intrusion detection systems. By adopting a holistic view, researchers can better anticipate and address potential vulnerabilities, thereby enhancing the overall security and reliability of their research endeavors.⁴

The processing phase in international research collaborations involves the manipulation and analysis of input data, where quality assurance mechanisms are crucial to maintaining data integrity. This phase is essential for ensuring the reliability and validity of research outcomes. Quality assurance and quality control are vital for preventing and correcting errors in data collection. Research data integrity is foundational for rigorous and reproducible research, requiring careful planning and management throughout the data lifecycle, including acquisition, analysis, and preservation.⁵

Standardization of methods is crucial to ensure consistent data handling across different collaborators, especially in international projects. Standardization of methods is paramount in ensuring consistent data handling across diverse collaborators, particularly in international projects where variations in protocols could lead to discrepancies. The European Network for Quality

² Zihad Hasan Joy et al., "Advanced cybersecurity protocols for securing data management systems in industrial and healthcare environments," *Global Mainstream Journal of Business, Economics, Development & Project Management* 4, no. 3 (2024), 25–38.

³ Tirumala Rao Vinnakota, "Systemic Assessment of Risks for Projects: A Systems and Cybernetics Approach," *2011 IEEE International Conference on Quality and Reliability*, 2011, 376–80.

⁴ Khanyisile Vilakazi and Funmi Adebesein, *A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies EPIc Series in Computing*, 2023; Yesem Kurt Peker, *Raising Cybersecurity Awareness among College Students*, 2016.

⁵ Rebecca Kush et al., "Implementing Single Source: The STARBRITE Proof-of-Concept Study," *Journal of the American Medical Informatics Association: JAMIA* 14, no. 5 (2007), 662–73.

Assurance in Higher Education (ENQA) underscores the significance of such standardization in facilitating cross-border cooperation and mobility within the European Higher Education Area.⁶ This standardization extends beyond mere data formats to encompass entire workflows and methodologies. Version control is necessary to manage multiple dataset iterations and analysis scripts, which can be complex across institutions and time zones. Computational resource management must balance powerful data processing capabilities with security considerations, particularly in cloud computing environments.

To address these challenges, researchers should implement standardized data processing workflows, use secure version control systems with robust access management, employ encrypted data storage and transmission protocols, and conduct regular security audits of data processing infrastructure.

The outputs of international research projects encompass not only the immediate results but also their broader impacts on the scientific community and society. Assessing the quality of these outputs requires sophisticated measurement tools and frameworks.⁷ From a cybersecurity perspective, the management of research outputs presents several challenges:

1. Intellectual property protection: Safeguarding novel findings and innovations, especially in collaborative projects with multiple stakeholders.
2. Embargoes and controlled release: Managing the timing and extent of result dissemination, particularly for sensitive or potentially dual-use research.
3. Long-term data preservation: Ensuring the security and integrity of research outputs over extended periods.

To address these challenges, institutions should consider implementing robust digital rights management systems, developing clear policies for result dissemination and embargo periods, and investing in secure, long-term data archiving solutions.

⁶ ENQA, "Quality Assurance and Internationalisation: State of Play and Perspectives for the Future," 2024, the website of European Network for Quality Assurance in Higher Education, May 8, 2024, <https://www.enqa.eu/publications/quality-assurance-and-internationalisation-state-of-play-and-perspectives-for-the-future>.

⁷ Ulven and Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education".

Strategies for cultivating a robust cybersecurity culture in academic settings are crucial for protecting sensitive data, research, and intellectual property in an increasingly digital educational landscape.

One of the most effective strategies is the implementation of comprehensive and ongoing cybersecurity awareness programs. These programs should be tailored to different stakeholder groups within the academic community, including students, faculty, staff, and administrators. Interactive e-learning modules that demonstrate the consequences of careless cyber habits can significantly increase awareness among college students. Such modules should cover topics such as password security, social engineering awareness, and safe browsing practices. Interactive e-learning modules that demonstrate the consequences of careless cyber habits can significantly increase awareness among college users, particularly when addressing fundamental security concepts and social engineering threats.⁸

Regular training sessions and workshops are essential components of a robust cybersecurity culture. These should be designed to keep all members of the academic community updated on the latest cyber threats and defense mechanisms. By conducting these sessions frequently, institutions can ensure that cybersecurity remains a top-of-mind concern for all stakeholders.

Fostering a sense of shared responsibility is crucial in building a strong cybersecurity culture. As emphasized by the Princeton University case study (ISACA, 2020), it's important to bridge the gap between awareness and genuine concern for cybersecurity. This can be achieved by connecting different audience segments with compelling stories and imagery that demonstrate the real-world impact of cyber threats.

Implementing a multi-faceted approach to skill development is also vital. A strategy that combines education, collaboration, research, and awareness to protect critical infrastructure. This holistic approach ensures that all aspects of cybersecurity are addressed within the academic environment. Leveraging diverse training delivery methods can enhance engagement and cater to different learning preferences. Implementing a multi-faceted approach

⁸ Jonathan Hobbs, "Cybersecurity Awareness in Higher Education: A Comparative Analysis of Faculty and Staff," *Issues in Information Systems* 24, no. 1 (2023), 159–69.

to skill development is vital. The Cybersecurity Awareness Framework for Academia emphasizes the importance of structured training modules (CATM) integrated into the academic curriculum, ensuring comprehensive coverage of security awareness topics.⁹

Finally, promoting collaboration between academic institutions and the private sector can facilitate knowledge sharing and the adoption of best practices. Such partnerships can provide valuable insights into real-world cybersecurity challenges and solutions, enriching the academic cybersecurity culture.

The Role of Digital Platforms in the Research Ecosystem

Digital platforms have revolutionized the modern research ecosystem by connecting multiple user groups through shared technological infrastructure. These platforms offer features such as modularity and extensibility, allowing for flexible component integration and expansion. Their role extends beyond technical functionalities to encompass economic and social interactions, fundamentally transforming how scientific collaborations are conducted and data is managed.¹⁰ Cloud computing has emerged as critical tools, enhancing the efficiency, security, and transparency of research processes. However, the adoption of these platforms also introduces new cybersecurity challenges that require careful consideration and mitigation strategies.

Figure 1 illustrates the complex web of cybersecurity challenges facing digital platforms in research ecosystems. The mind map effectively visualizes five major interconnected areas of concern: Digital Divide, Regulatory Compliance, Data Breaches, IP Ownership, and Unauthorized Access. Each of these core challenges branches into specific issues that require careful consideration. The Digital Divide node highlights resource inequalities and limited access to tools, while Regulatory Compliance emphasizes jurisdictional conflicts and fragmented policies. Data Breaches point to centralized data risks and sensitive information exposure. IP Ownership addresses credit disputes and blurred attribution, which is particularly relevant in colla-

⁹ Mohammed Khader, Marcel Karam, and Hanna Fares, "Cybersecurity Awareness Framework for Academia," *Information* 12, no. 10 (2021).

¹⁰ Mark de Reuver, Carsten Sørensen, and Rahul C. Basole, "The Digital Platform: A Research Agenda," *Journal of Information Technology* 33, no. 2 (2018).

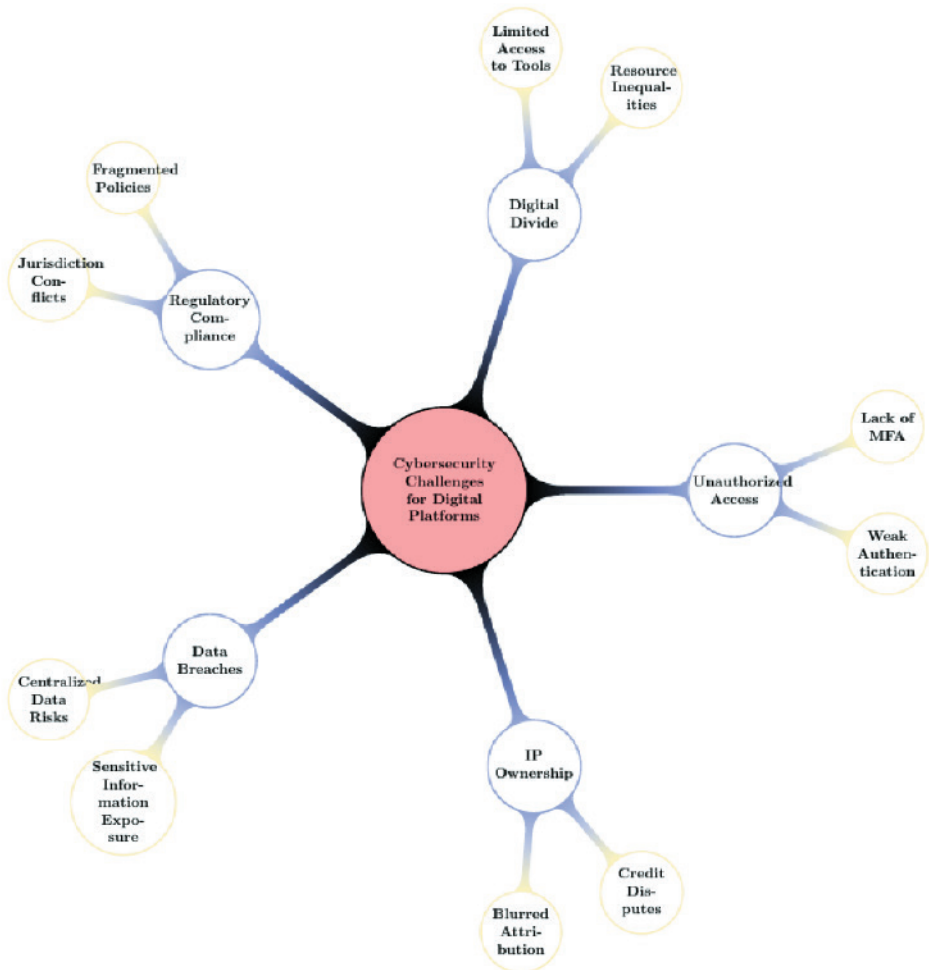


Figure 1. Cybersecurity Challenges in Digital Research Platforms. A Mind Map of Key Vulnerabilities.

borative research environments. The Unauthorized Access branch identifies weak authentication and lack of multi-factor authentication (MFA) as critical vulnerabilities. This visualization complements the discussion of digital platforms in the research ecosystem by mapping out the specific cybersecurity challenges that need to be addressed when implementing and managing digital research platforms.

Digital platforms significantly enhance scientific productivity by streamlining workflows and reducing barriers to collaboration. Cloud-based tools

such as Jupyter Notebooks enable researchers to share not only data but entire analytical workflows, promoting reproducibility and accelerating the pace of discovery.¹¹ This level of transparency and collaboration was previously unattainable in traditional research paradigms. Platforms such as the Open Science Framework (OSF) provide comprehensive infrastructure for managing entire research projects, from preregistration to data archiving. This approach ensures that scientists with diverse specialties can contribute at various stages of the research process, maximizing the utilization of expertise across disciplines.¹²

While digital platforms offer numerous benefits, they also present significant risks that must be addressed. The centralization of research data increases the potential impact of data breaches, potentially exposing sensitive information to unauthorized access.¹³ The open nature of many platforms can blur the lines of intellectual property ownership, requiring scientists to navigate complex issues of attribution and credit.¹⁴ Additionally, the digital divide may exacerbate existing inequalities in the scientific community, potentially marginalizing researchers from resource-limited institutions or regions.¹⁵

A critical yet often overlooked aspect of digital platforms in research ecosystems is the inherent power asymmetry between platform owners and complementors, which introduces additional cybersecurity considerations. Platform owners possess disproportionate control over the technological infrastructure, governance mechanisms, and data access policies, creating a significant power imbalance in the research ecosystem. This asymmetry becomes particularly concerning when platform owners can unilaterally enforce changes in security protocols or access conditions that may impact ongoing research collaborations. The relationship between platform owners and rese-

¹¹ Thomas Kluyver et al., "Jupyter Notebooks—a Publishing Format for Reproducible Computational Workflows," *International Conference on Electronic Publishing*, 2016.

¹² Erin D. Foster and Ariel Deardorff, "Open Science Framework (OSF)," *Journal of the Medical Library Association* 105, no. 2. (2017), 203–206.

¹³ Katherine Akers and Jennifer Doty, "Disciplinary Differences in Faculty Research Data Management Practices and Perspectives," *International Journal of Digital Curation* 8, no. 2. (2013), 5–26.

¹⁴ Thomas Lemieux, "Big Data, Little Data, No Data: Scholarship in the Networked World," *Canadian Journal of Communication* 42, no. 1. (2017).

¹⁵ Louise Bezuidenhout et al., "Beyond the Digital Divide: Towards a Situated Approach to Open Data," *Science and Public Policy* 44, no. 4. (2017), 464–475.

arch complementors is further complicated by the shared objective of providing value to the scientific community while maintaining robust security measures. These power dynamics can affect how security protocols are implemented, potentially creating vulnerabilities if complementors lack sufficient autonomy to implement additional security measures or if platform owners prioritize scalability over security concerns. Understanding and addressing these power asymmetries is crucial for developing comprehensive cybersecurity strategies that protect both platform integrity and research data while ensuring equitable participation in international research collaborations.

To mitigate these risks, the scientific community must adopt a proactive approach. Implementing robust cybersecurity measures, including end-to-end encryption and multi-factor authentication, is crucial for protecting sensitive research data. Clear guidelines for data sharing and intellectual property rights in collaborative digital environments must be developed. Investing in open-source platforms and infrastructure can reduce dependence on commercial entities and promote equitable access. Providing training in digital literacy and data management ensures that all scientists can effectively navigate and utilize digital platforms. Encouraging the development of AI-powered tools can help researchers manage information overload and identify relevant collaborations.

By addressing these challenges, the scientific community can harness the full potential of digital platforms while mitigating associated risks. This balanced approach will ensure that the complementary nature of scientists in digital environments continues to drive innovation and discovery in an increasingly interconnected world. As digital platforms continue to evolve, ongoing research and adaptation of best practices will be essential to maintain the integrity and security of international research projects while maximizing the benefits of these transformative technologies.

Summary

This article explores the critical intersection of cybersecurity, international scientific collaboration, and digital research platforms. It examines the complex interplay between open scientific practices and security requirements

in academic environments, focusing on three key components: input quality and data sources, data processing methods, and the potential impact of research outputs. The study identifies critical vulnerabilities in current research workflows and proposes strategies for cultivating a robust cybersecurity culture in academic settings. These strategies include implementing comprehensive cybersecurity awareness programs, conducting regular training sessions and workshops, fostering a sense of shared responsibility, and promoting collaboration between academic institutions and the private sector. The article also highlights the transformative role of digital platforms in the research ecosystem, emphasizing their ability to enhance scientific productivity while introducing new cybersecurity challenges that require careful consideration and mitigation strategies. By addressing these challenges and adopting a balanced approach, the scientific community can harness the full potential of digital platforms while safeguarding the integrity and security of international research projects in an increasingly interconnected world.

Policy Recommendations

Academic institutions should implement comprehensive cybersecurity awareness programs tailored to different stakeholder groups, including regular training sessions and workshops that address emerging cyber threats. Research institutions must establish clear data governance frameworks that balance open science principles with robust security measures, including standardized protocols for data sharing and access control. Government agencies should develop and enforce consistent cybersecurity standards for international research collaborations while providing adequate funding for security infrastructure and training programs. Digital platform providers must implement enhanced security features, including end-to-end encryption and multi-factor authentication, while ensuring equitable access across the global research community. International cooperation between academic institutions and private sector cybersecurity experts should be promoted to facilitate knowledge sharing and the adoption of best practices.

Bibliography

- Akers, Katherine and Jennifer Doty. "Disciplinary Differences in Faculty Research Data Management Practices and Perspectives." *International Journal of Digital Curation* 8, no. 2. (2013): 5–26.
- Bezuidenhout, Louise, Sabina Leonelli, Ann Kelly and Brian Rappert. "Beyond the Digital Divide: Towards a Situated Approach to Open Data." *Science and Public Policy* 44, no. 4. (2017): 464–475.
- European Network for Quality Assurance in Higher Education. "Quality assurance and internationalisation: state of play and perspectives for the future." ENQA, May 8, 2024. <https://www.enqa.eu/publications/quality-assurance-and-internationalisation-state-of-play-and-perspectives-for-the-future> (access at 16.07.2025).
- Foster, Erin D. and Ariel Deardorff. "Open Science Framework (OSF)." *Journal of the Medical Library Association* 105, no. 2. (2017): 203–206.
- Hobbs, Jonathan. "Cybersecurity Awareness in Higher Education: A Comparative Analysis of Faculty and Staff." *Issues in Information Systems* 24, no. 1 (2023): 159–69.
- Joy, Zihad Hasan, Siful Islam, Md Atiqur Rahaman and Md Haque. "Advanced cybersecurity protocols for securing data management systems in industrial and healthcare environments." *Global Mainstream Journal of Business, Economics, Development & Project Management* 4, no. 3 (2024): 25–38.
- Khader, Mohammed, Marcel Karam and Hanna Fares. "Cybersecurity Awareness Framework for Academia." *Information* 12, no. 10 (2021).
- Kluyver, Thomas, Benjamin Ragan-Kelley, Fernando Pérez, Brian E. Granger, Matthias Bussonnier, Jonathan Frederic, Kyle Kelley et al. "Jupyter Notebooks—a Publishing Format for Reproducible Computational Workflows." *International Conference on Electronic Publishing*, 2016.
- Kush, Rebecca, Liora Alschuler, Roberto Ruggeri, Sally Cassells, Nitin Gupta, Landen Bain, Karen Claise, Monica Shah and Meredith Nahm. "Implementing Single Source: The STARBRITE Proof-of-Concept Study." *Journal of the American Medical Informatics Association: JAMIA* 14, no. 5 (2007): 662–73.
- Lemieux, Thomas. "Big Data, Little Data, No Data: Scholarship in the Networked World." *Canadian Journal of Communication* 42, no. 1. (2017).

- Peker, Yesem Kurt. "Raising Cybersecurity Awareness among College Students." 2016.
- Reuver, Mark de, Carsten Sørensen and Rahul C. Basole. "The Digital Platform: A Research Agenda." *Journal of Information Technology* 33, no. 2 (2018).
- Ulven, Joachim B. and Gaute Wangen. "A Systematic Review of Cybersecurity Risks in Higher Education." *Future Internet* 13, no. 39 (2021).
- Vilakazi, Khanyisile and Funmi Adebisin. *A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies EPiC Series in Computing*, 2023.
- Vinnakota, Tirumala Rao. "Systemic Assessment of Risks for Projects: A Systems and Cybernetics Approach." *2011 IEEE International Conference on Quality and Reliability*, 2011, 376–80.