Proceedings of the 5th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/112/2024.17910

Information Security Management at the University: A Critical Review of Recent Studies

Yahong Jiang[1,a,*]

[1]*School of Professional Studies, New York University, New York, United States*
a. Yj2808@nyu.edu
**corresponding author*

Abstract: As global cyber threats continue to escalate, particularly with the increasing frequency of attacks targeting academic institutions, information security management (ISM) has become imperative for safeguarding the confidentiality and integrity of personal and research data within universities. This study examines the increasingly strategic role of information security management (ISM) in universities that face growing threats to personal and research data. This paper identifies key trends, methodological approaches, and research gaps within university ISM by reviewing research published over the past decade. Findings reveal that, despite the critical importance of ISM, the field still needs to be explored, with significant opportunities for further research in areas such as human factors, organizational culture, and information security behaviors. This research provides a comprehensive overview for IT professionals and university information security managers. It offers insights into the evolving ISM landscape in higher education and highlights new avenues for future investigation.

Keywords: University, Information security management, Cybersecurity Challenges.

1. Introduction

Information is a critical asset in modern organizations, essential for operations and a key driver of competitiveness [1-2]. Given its pivotal role, it has become a primary target for cyber threats, from viruses and worms to data breaches. Statista's 2023 report indicates that over 6 million data records were compromised in the first quarter alone, emphasizing the severity of these risks [3]. With U.S. data breaches averaging $9.48 million in damages [4], organizations face significant financial, legal, and reputational harm. The rapid growth of information technology further complicates security by expanding system access beyond IT professionals to unauthorized users, escalating the need for comprehensive security measures. Consequently, physical protection alone is insufficient. Organizations must implement an information security management system (ISMS) to protect all resources involved in information processing—facilities, personnel, computers, and media [5-6]. Information security management (ISM) refers to the processes, policies, and technical measures used to protect information systems and assets from unauthorized access, disruption, theft, or modification [7]. ISM helps mitigate various threats and share organizational information in a trustworthy way. As organizations increasingly rely on leveraging technological knowledge, effective information security management has become a strategic imperative, drawing increasing attention from practitioners and scholars, ensuring the protection of critical assets, and fostering sustainable organizational success.

DOI: 10.54254/2755-2721/112/2024.17910

In today's academic landscape, information security management is essential for safeguarding sensitive data, intellectual property, and academic integrity. As universities expand digital communication and infrastructure (e.g., Brightspace, swipe card access systems), they face heightened risks of data breaches and privacy issues, particularly for academic and personal information [8]. Universities also possess assets that attract hackers, such as student personal data (e.g., SSNs), computational power for cryptocurrency mining, intellectual property, and valuable research data. The frequency of information security incidents in higher education is rising globally (see Table 1). In this digital age, robust information security management is critical for universities.

Table 1: Information security breaches at universities in 2023

Date	University	Data Breach
7/2023	University of Minnesota	• Database Hack • 7M+ social security number • Data stolen dates to 1989
9/2023	University of Georgia	• Unauthorized access • Third-Party Software Vulnerability
9/2023	Baruch College	• Cyberattacks
11/2023	North Carolina Central University	• Disruptive cyberattack • Internal human error

(Source from Google)

Previous literature has primarily addressed information security management (ISM) as a technical issue [9], with a focus on technical solutions [10], information security policy development [11-13], and fostering a security-aware culture [14-16]. While these studies provide valuable insights for building a security-conscious workforce, they overlook academic institutions' unique cultural and structural dynamics. Although notable progress has been made in the technical, policy, and cultural dimensions of ISM, research addressing the managerial aspects of ISM in universities remains limited [17-19]. This study thus aims to explore the managerial dimensions of ISM within the university setting, where challenges such as open access, diverse users, and data sensitivity demand specialized approaches.

Scholarly research on university-specific information security management (ISM) remains relatively limited, though its importance has recently grown [20-21]. This review provides a comprehensive examination of ISM studies within academic institutions, highlighting the critical role of ISM in helping universities navigate digital complexities while protecting sensitive data and maintaining the integrity of their educational missions.

2. Methodology

This study applies a grounded theory approach [22] to synthesize existing knowledge on the role of management in information security within academic institutions. The methodology follows three key steps:

Step 1: Establish Research Questions: Based on the framework [23], we first developed research questions to guide our investigation of university information security management. The questions are as follows: (a) What are the primary topics explored in the research? (b) How is information security management studied in the literature in terms of year, location, sample, and methodologies? (c) Which topics are deemed essential or impactful for further study?

Step 2: Literature Search and Selection: We conducted a systematic literature search using keywords such as "information security management," "cybersecurity management," "university," and "college" across multiple databases: Scopus, Web of Science, Google Scholar, AIS Library, and

DOI: 10.54254/2755-2721/112/2024.17910

IEEE Xplore. To ensure relevance and rigor, we included only peer-reviewed articles published within the last ten years, resulting in a selection of 67 articles. The flowchart in Figure 1 illustrates the process of identifying qualified studies.

Step 3: Data Analysis: We analyzed the selected literature by applying grounded theory coding techniques to identify recurring themes and management roles within information security. That involves categorizing themes based on managerial practices, policy development, and cultural impact in academic settings. The analysis revealed that various managerial aspects significantly shape effective information security management in universities.

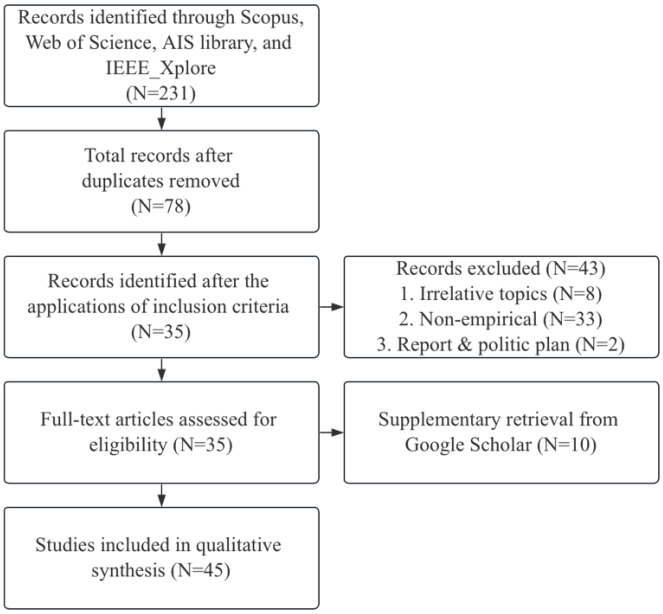

Figure 1: Procedural outline of literature selection

3. Results

The results comprehensively analyze key findings in university information security management (ISM) research, detailing core topics, geographic distribution, sample populations, and methodologies to understand ISM challenges unique to universities. This section highlights primary focus areas and identifies research gaps, offering insights into the current landscape and directions for future exploration in higher education.

3.1. Key Topics in University ISM Research

The study summarizes the primary topics and patterns in information security management (ISM) research related to universities. The analysis shows that 42% of the studies focus on risk management frameworks and principles within colleges, highlighting a strong emphasis on strategies to mitigate institutional risks. In contrast, only 5% of the center of the paper is on governance-related aspects of ISM, such as information security policies, cyber behaviors, risk management frameworks or standards, culture or awareness, etc. See Table 2 for further details. Additionally, an assessment of recurrent keywords across the reviewed papers reveals key topical patterns, including "information security," "information security policy," "information security management system," "security threat," and "university." This clustering of keywords suggests that these themes are central to university-focused ISM research. Interestingly, only three papers specifically address cybersecurity breaches, demonstrating a relatively low focus on this area and a diversity of subtopics. This finding

DOI: 10.54254/2755-2721/112/2024.17910

suggests that cybersecurity breaches may be an underexplored topic in the context of university ISM research.

Table 2: The main topics in the literature [35]

Topic	Descriptor	Sub-topics	Frequency (papers)
Risk management frameworks and standards [24-25]	Frameworks for managing information security as a risk often stem from organizational policies, which may be based on international standards (e.g., ISO 27001).	Framework development, implementation, assessment; IS management systems; risk and vulnerability assessment, etc.	17
Information security policies [26-27]	Providing the foundation for risk management frameworks, defining goals, implementation, and compliance in information security.	Formulation, implementation, compliance; policy presence; alignment with organizational strategy; adherence to ISO 27001.	5
Sociotechnical holistic approach [28]	Both technical (e.g., IT architecture) and social components (e.g., training), extending beyond IT departments.	End-users' role in information security; security as everyone's responsibility; IT security shaped by organizational dynamics and human factors.	5
Technical solutions [29-30]	An engineering, solution-focused approach to information security, primarily addressing cyber-defense effectiveness.	Security threats, layered controls, web application security, campus network protection.	4
Cyber-behaviors [31]	End-point vulnerability is primarily driven by human factors (e.g., intentions, perceptions)	Lifestyle routines, protection motivation, outcome expectations, social networking habits.	4
Culture and awareness [32]	as part of organizational culture, is shaped by employee awareness, top management support, and end-user cyber behaviors.	Information security training; cultural approach to youth information security.	3
Governance [33-34]	How organizations plan and manage information security	Managed security services; outsourcing; decentralization.	2

3.2. Analysis of Trends, Populations, and Methodologies

Figure 2 shows a steady increase in scholarly publications on information security management (ISM) in universities over recent years, reflecting growing interest in this area. Geographic Distribution: The studies demonstrate significant geographic diversity, with the majority conducted in the US (6 studies), followed by Malaysia (4), China (4), Indonesia (3), Canada (2), and New Zealand (2). Sample Populations: The literature utilizes a range of sample populations, including students, IT staff, and administrative personnel. Notably, 25 studies evaluated ISM effectiveness, 7 analyzed students'

DOI: 10.54254/2755-2721/112/2024.17910

unsafe behaviors, and 5 focused on university information systems. Research Methodologies: Methodological approaches are varied. Conceptual frameworks are the most common, complemented by descriptive statistics (e.g., assessing guideline implementation), regression analysis, and structural equation modeling. Data collection methods primarily include surveys, questionnaires, interviews, and laboratory tests, allowing for in-depth analysis of ISM practices in higher education institutions. These findings underscore the diversity of ISM research in universities, highlighting a range of geographic, demographic, and methodological approaches used to explore information security in academic settings.

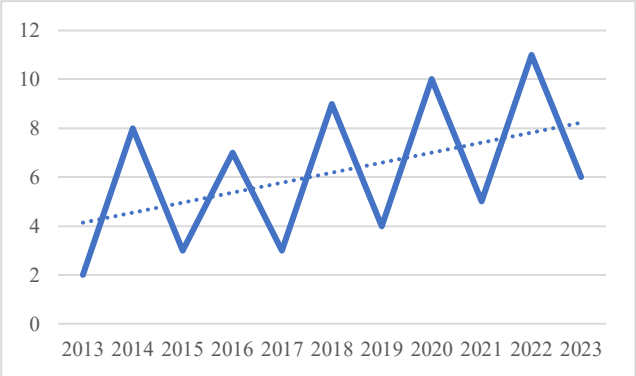

Figure 2: Number of publications per year with trend

3.3. Strategic Challenges of ISM in Universities

The findings reveal that much of the ISM literature in universities has a limited focus on the strategic significance of managing information security in academic settings. Notably, 13 studies recognize universities as knowledge-intensive organizations with high complexity, which increases their susceptibility to cyberattacks and poses potential financial risks. Several researchers also utilized 'vulnerability' as a key indicator to examine ISM challenges in these institutions, emphasizing areas where universities may be especially exposed. Additionally, four studies highlight the strategic value of safeguarding academic achievements and intellectual property, such as patents, in university settings. Other papers explore aspects unique to ISM in higher education, including the widespread adoption of BYOD (Bring Your Own Device) and the openness of universities as multimodal learning and innovation hubs.

4. Discussion

This study investigates information security management (ISM) in universities, where organizational and managerial aspects are increasingly emphasized. Consistent with broader literature [7], universities are applying structured security architectures to protect data and teaching systems, highlighting the importance of ISM in academia. Additionally, our review suggests a complex ISM environment within universities, characterized by varied perspectives among students, faculty, and administrators, which introduces unique cultural dynamics around information security. Exploring these diverse viewpoints—such as differing levels of awareness, perceptions, and behaviors—presents an intriguing area for future research.

The literature review reveals that ISM in universities is an emerging topic with many gaps in empirical testing, conceptual frameworks, and robust quantitative methods, supporting the need for further research. Southeast Asian scholars, alongside U.S. researchers, have contributed significantly to this area, with 13 studies focused on university ISM. However, some information-sharing barriers remain across regions (e.g., limited use of open-access databases). Some researchers have attributed

DOI: 10.54254/2755-2721/112/2024.17910

the limited focus on university ISM to the traditionally open, collaborative architecture of higher education institutions, which facilitates information exchange and connects vast IT systems. However, the expanding value of universities as repositories of intellectual property (IP) and personal data, along with their culture of academic innovation, makes them increasingly attractive targets for cyber threats.

Significant gaps in university ISM literature remain. Critical areas for future research include examining information security culture within academic institutions, mainly how awareness and attitudes vary among students, faculty, and administrators. Comparative studies across different regional and international universities would also provide valuable insights. Practically advancing this research would benefit professionals such as Chief Information Security Officers (CISOs), Certified Information Systems Auditors (CISAs), and university end-users by informing ISM practices tailored to the unique environment of higher education institutions.

5. Conclusion

This study uses a grounded theory approach to analyze information security management (ISM) in universities, emphasizing the unique managerial complexities these institutions face in addressing information security challenges, such as academic information breaches. Our analysis identified several key topics within the literature, revealing that ISM research in universities is still in its early stages, having only begun to develop significantly since 2014. That highlights an urgent need for further exploration and novel research. In summary, universities' open architecture, diverse organizational cultures, and varied end-users pose unique challenges for ISM. This study provides IT staff and university information security professionals with a holistic overview of the current research landscape, offering valuable insights to guide future improvements in information security practices within higher education institutions.

References

[1] *Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.*

[2] *Humphreys, E. (2011). Information security management system standards. Datenschutz und Datensicherheit-DuD, 35, 7-11.*

[3] *Ani Petrosyan (2023) Number of data records exposed worldwide from 1st quarter 2020 to 1st quarter 2023. https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/, accessed 7 December 2023.*

[4] *Mark Stone (2023) Cost of a data breach 2023: Geographical breakdowns. https://securityintelligence.com/articles/cost-of-a-data-breach-2023-geographical-breakdowns/, accessed 7 December 2023.*

[5] *Almasalha, H. M., Taha, N. N., & Abumqibl, A. (2021). The status quo of information security from the perspective of information technology staff in Jordanian University Libraries. Journal of Information Security and Cybercrimes Research, 4(1), 55-80.*

[6] *Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information security behaviors among employees. International Journal of Academic Research in Business and Social Sciences, 9(6), 560-571.*

[7] *Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International journal of information management, 36(2), 215-225.*

[8] *Borgman, C. L. (2018). Open data, grey data, and stewardship: Universities at the privacy frontier. Berkeley Technology Law Journal, 33(2), 365-412.*

[9] *Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ism) practices: Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management, 14, 225-239.*

[10] *Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.*

[11] *Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38(1), 60-80.*

[12] *Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems.*

DOI: 10.54254/2755-2721/112/2024.17910

[13] D'Arcy, J., & Teh, P. L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. Information & Management, 56(7), 103151.
[14] Da Veiga, A. (2015). An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture. In HAISA (pp. 95-107).
[15] Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & security, 88, 101640.
[16] Kori, D., & Naik, R. (2023). Information Security Awareness Among Postgraduate Students: A Study of Mangalore University. In Handbook of Research on Technological Advances of Library and Information Science in Industry 5. 0 (pp. 270-286). IGI Global.
[17] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security, 66, 40-51.
[18] Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224.
[19] Hui, S. C., Kwok, M. Y., Kong, E. W., & Chiu, D. K. (2023). Information security and technical issues of cloud storage services: a qualitative study on university students in Hong Kong. Library Hi Tech.
[20] Marks, A. A. (2007). Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research. University of Salford (United Kingdom).
[21] Okibo, B. W., & Ochiche, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa–Kenya. International Journal of Management Excellence, 3(1), 336-349.
[22] Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. European journal of information systems, 22(1), 45-55.
[23] Papaioannou, D., Sutton, A., & Booth, A. (2016). Systematic approaches to a successful literature review. Systematic approaches to a successful literature review, 1-336.
[24] Joshi, C., & Singh, U. K. (2017). Information security risks management framework–A step towards mitigating security risks in university network. Journal of Information Security and Applications, 35, 128-137.
[25] Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. (2021). Risk management in sustainable smart cities governance: A TOE framework. Technological Forecasting and Social Change, 167, 120743.
[26] Awang, N., Samy, G. N., Hassan, N. H., Maarop, N., Magalingam, P., & Kamaruddin, N. (2020, May). Identification of information security threats using data mining approach in campus network. In Journal of Physics: Conference Series (Vol. 1551, No. 1, p. 012006). IOP Publishing.
[27] Ismail, W. H. B. W., & Widyarto, S. A. (2016, April). Formulation and development process of information security policy in higher education. In Proceedings of the 1st International Conference on Engineering Technology and Applied Sciences, Afyonkarahisar, Turkey (pp. 21-22).
[28] Navarro-Bringas, E., Bowles, G., & Walker, G. H. (2020). Embracing complexity: A sociotechnical systems approach for the design and evaluation of higher education learning environments. TheoreTical issues in ergonomics science, 21(5), 595-613.
[29] Paiziaihemaiti, A., & Arxiden, A. (2016, June). Research on network information security analysis and prevention strategies of campus network in Xinjiang Uygur Medical College. In 2016 6th International Conference on Machinery, Materials, Environment, Biotechnology and Computer (pp. 94-100). Atlantis Press.
[30] Khan, A., Ibrahim, M., & Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. International Journal of Information Management Data Insights, 1(2), 100015.
[31] Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. Computers in Human Behavior, 73, 394-402.
[32] Saraçlı, S., & Erdoğmuş, A. (2019). Determining the effects of information security knowledge on information security awareness via structural equation modelings. Hacettepe Journal of Mathematics and Statistics, 48(4), 1201-1212.
[33] Wang, J. (2017). Information Security Governance in Colleges and Universities. DEStech Transactions on Economics, Business and Management, (icem). https://doi. org/10.12783/dtem/icem2017/13206.
[34] Liu, C. W., Huang, P., & Lucas, H. (2017). IT centralization, security outsourcing, and cybersecurity breaches: evidence from the US higher education.
[35] Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350-357.