INFORMATION SECURITY ASPECTS IN HIGHER EDUCATION

UDC: [378.14:004.056.5]:005.342
DOI: https://doi.org/10.53486/tids2025.16

KRASIMIR SHISHMANOV
Professor, PhD
k.shishmanov@uni-svishtov.bg
ORCID ID: 0000-0001-9874-2149

EMIL TSANOV
Head Assist. Prof., PhD
e.tsanov@uni-svishtov.bg
ORCID ID: 0009-0003-0957-1301

ISKREN TAIROV
Head Assist. Prof., PhD
i.tairov@uni-svishtov.bg
ORCID ID: 0000-0002-2971-5451

Abstract. Recent studies indicate that information security plays an increasingly critical function in businesses today. Higher education is not an exemption. The growing number of safety incidents reported by higher education organizations in the past few years exemplifies the significance of privacy, reliability, and information accessibility in universities. The current review attempts to improve the authors' grasp of the views, methodology, and tendencies that define this emerging field of study. A literature review is conducted, and a direction for future research is suggested. The article suggests the fact that data protection in higher education is a profoundly unstudied topic. Other studied subjects include data safety habits, study evaluations of management information security in areas other than higher education, comparing studies between educational institutions, as well as security monetary theory and administration.

Keywords: smart cities, security, measures, deep learning.

Classification JEL: L86

INTRODUCTION

Recently, the advent of technological innovations has provided individuals, companies, and society as entirety with new opportunities. Improved chances for government and business enterprises to collect, analyze, and control data, as well as produce novel insights have appeared, becoming handling information an essential corporate component. The dominant alternatives given by the age of computers have led to novel protection requirements, which manifest in a variety of means: an environment of constantly shifting IT techniques; new laws for protecting data, and the emergence of ethical difficulties. Each of the demands has a cohesive source: a computerized, allowed, and social response to the increasing incidence of events involving information security.

Data safety is based on the principles of privacy, reliability, and accessibility of information (Whitson, 2003), and it has grown in significance and effect on present-day organizations. The rise in IT security expenses relates to the growing relevance of security concerns as a component in company decision-making, including topics such as the responsibilities of the corporate authority (Curry, 2017), a data security culture, and managerial support.

Because of the acknowledged importance of privacy and security in computerized assessments (Lowry et al., 2017), academic research remains behind, and subjects like the managerial approaches for information assurance awareness of information security (Parsons et al., 2017) and the importance of psychological factors have only lately become subjects of research. In general, the scientific community recommends additional studies on information security's organizational and executive parts to supplement the conventional, scientific tackle (Soomro et al., 2016). The current study answers these inquiries and investigates the managerial components of information security, emphasizing a specific field: higher education.

THEORETICAL BACKGROUND

Higher education institutions are located at among the greatest congested crossroads of the global digital economy. Such open-by-design (Borgman, 2018), decentralized, multi-stakeholder, ephemeral systems are typically linked with information technology, studies, and creativity. Students, educators, employees, and arrivals use higher education computer networks to acquire and generate knowledge in a variety of ways, including their cellphones and wearables (bring-your-own-device, BYOD), business desktops and notebooks, testing detectors, and scroll authentication mechanisms. Data transfer between educational institutions as organizations and their different consumers is ongoing (Chapman, 2019).

Higher education institutions, like many innovative companies, are expanding online, increasing their vulnerability to assaults by hackers and mandating continual surveillance and confidentiality of activities. However, the higher education setting appears to have an inherently unique connection to the security of information due to its multilayered method, inflexible construction, and central oversight. Most institutions lack the capacity for offering centralized safety measures, so substantial licensing of information security is frequently the favored alternative (Liu et al., 2017). The fact that this happens in one conjunction allows for quicker and more successful responses to cyber-attacks, but it also expands educational organizations' digital footprints and necessitates sufficient administration and contract administration.

A further challenge is that various kinds of customers in colleges have different levels of expertise in information security standards, making education efforts difficult at best. This last component is compounded by a historically high level of turnover and a typically lax perception of information security. Based on a threat actor's perspective, the period of educational institutions not owning any appealing resource is over: with computing resources (utilized, for instance, for launching distributed-denial-of-service assaults or, lately, for "mining" digital currencies) to private information, to trademarks, and some research information, educational institutions are swiftly ascending hackers' curiosity specifies.

As a consequence of all these complicated factors, the quantity of known information security catastrophes in higher education is increasing globally (Chapman, 2019), with some high-profile cases reaching the news lately. University research into the administration of information security in higher education is yet in its early stages (Okibo, 2014). At the very same time, previous work (Doherty et al., 2009) has shown that information security on campuses varies from other organizations, making managing information security in higher education a distinct studying subject. To determine and evaluate the latest developments in this newly developing area of investigation, the current paper presents a comprehensive assessment of academic studies on information security administration in higher education.

METHODOLOGY

The current investigation was divided into six sections: establish, investigate, choose, evaluate, present, and design.

Initially, an examination strategy centered on the study's theme was created, and research ideas were developed:

- Topics related to information security management in higher education;
- Literature study on security management in higher education.
- Importance of information security management in higher education.
- Recommendations for future research.

Secondly, the extent of the area, resources, and keywords were specified. The analysis was limited to higher education, information security, and computer science. In these instances, a search for records was performed using terms established during the review's preparation stage, according to the individual understanding of the research and a study of relevant works (Schatz & Bashroush, 2017). By narrowing the results to particular areas and putting the word management in the key phrase search, organizational and management difficulties were highlighted while an academic focus was spared. Small modifications have been implemented to the search phrases to account for the various possibilities for searches in datasets. Where achievable, the keywords, abstract, and title were investigated to confirm that the query's scope was consistent. To guarantee systematicity, all types of articles were initially examined regardless of sections such as publisher status, research methodology, or location.

Third, relevant studies were discovered using numerous characteristics to ensure applicability and quality (Pare et al., 2016). The initial round of removing focused on mathematical components: results were pared out by considering only published research and conference proceedings, which indicate rigorous methodology; papers in languages besides English were eliminated, as had been copies throughout records. The next phase of filtration concentrated on specific information elements: positive results were removed when, for instance, the phrases "college" or "higher education" reoccurred in the abstract merely as writers' connection information or for rights reasons (Wolfswinkel et al., 2013). The final phase of arranging focused on the most important parts: a broad study of summaries led to the elimination of documentation outside the area. A couple of articles from journals were also removed because they looked to have been mechanically transferred to English from another tongue, causing significant problems with accessibility and understanding. Finally, one manuscript was removed since it was very similar to another manuscript by the same creators, who most likely plagiarized their original material. Following this processing, a total of 18 articles were ultimately chosen.

Fourth, processing was carried out by analyzing the text of the examined literature with the research questions as guides.

Fifth, the findings of the evaluation were organized and reported.

Sixth, a paradigm of information security in higher education is suggested.

RESULTS

The initial step in the research process was to determine which subjects are most often referred to by researchers studying information security management at universities. Among the evaluated documentation, almost half of the selected literature focuses on researching risk management

guidelines and regulations used in universities to assure information security control and a small part of the investigated papers addressed administration of information security systems as a key subject.

The following stage sought to establish that information security management is an area of interest at universities. The results revealed that the majority of studies gave barely any rationale for studying information security management in higher education. Some studies identified institutions as accessible, multifaceted systems with a complicated structure that could raise susceptibility to information compromises. Two publications viewed universities as knowledge-intensive organizations for whom knowledge preservation is strategically important. Half of the researchers investigated the peculiarity of information security management in higher education, demonstrating its significance according to these considerations:

- Higher education institutions offer different computer systems that promote innovation and leadership and equilibrium of cultural and technological diversity with commercial and company requirements.
- Universities must secure the anonymity, honesty, and timeliness of legal records, such as graduation certificates.
- IT innovations and a BYOD attitude are widely used at schools.
- Higher education institutions are experiencing an increase in recorded privacy violations.
- Universities are open innovation engines and institutions of society.
- Universities and colleges' internet pages have turned into a focus for criminals in response to fragile information security technologies.
- Universities have usually been considered uncertain from an IT viewpoint.
- Universities are going through developing enrollment, making them more susceptible as organizations.
- Universities keep broad amounts of hard-copy products.

Multiple researchers focused on academics as consumers of college networks, investigating networking practices, sensitivity to risky websites, and susceptibility as a measure of managing information security success.

The fourth work stage synthesized proposals for future study in the subject of information security management at institutions. Overall, the examined publications made few or no specific suggestions for further study on the topic. Within those investigations that identified topics for additional research, scientists advocated using universities as an intermediary for examining security issues in public companies or as a standard for doing so in smaller enterprises. Other sectors proposed examining an information security management system designed for college surroundings, exploring the relationship among information security policies and university employees' tactical papers, or figuring out the way a policy on appropriate use might be relevant to higher education.

Likewise, several studies called for a broader comparison of managing information security among universities. Human factor evaluation was another potential field for further study, particularly in the areas of unintentional loss of data, end-user opinions on cyber-behaviors, the function of cyber-routines in the offender-offender dynamic, along with goals to prevent malicious software while employed at the place of employment and working from their homes.

MODEL

Information security encompasses safety concerns in all types of data handling and can be thought of as a method of securing data in order to ensure accessibility, privacy, honesty, and responsibility (SIS, 2003; ISO/IEC, 2005a). The essential concepts of information security include privacy, reliability, and accessibility (Ahlfeldt et al., 2007). These are known as CIAs. Confidentiality relates to protecting records from improper use. Integrity is characterized as safeguarding from unwanted shifts, and availability involves the expected utilization of items during the stipulated time frame. It has been contended and asserted that more elements ought to be added to the concept of information protection. SIS (2003) includes obligation as an additional factor in the security of data, building on BS 7799 (2002), ISO/IEC 17799 (2005a), and ISO/IEC 27002 (2005b). Accessibility entails understanding ways to trace performed work down to a particular individual. A third party is specifically deemed responsible and held accountable for the protection of something or a collection of services. The focus here is on individuals and their own accountability. All four of these features demand combined technical and managerial safety precautions. Administration privacy refers to the administration of the safety of information, including tactics, procedures, evaluations of risks, and others. In addition, the preparation and execution in the security field necessitate an organized approach. This aspect of total security is thus structural in nature, affecting the entire firm. It is geared toward what the overall safety guidelines would be. Practical protection is concerned with the steps to be performed to meet the total criteria (Dark & Shanks, 2002). Practical security can be separated into two categories: building safety and security for information technology. Physical safeguarding, for example, covers the actual safeguarding of knowledge storage and alarms, whereas IT security relates to ensuring the safety of information in technical information systems. IT safety can subsequently be classified into two categories: security of computers and safety of communication. Information technology safety protects infrastructure and its contents, whereas security for communication protects systems as well as different devices used to convey info across machines (Bjorck & Yngstrom, 2001).

To more fully comprehend how these features and safety safeguards interact, a model of information safety was created and employed in the first research (see Figure 1). The model's goal is to concisely convey what information security entails. The model includes the concepts and descriptions provided above.

The primary notion, the safety of information, is located at the center. The four traits are arranged at the highest level and symbolize the safety of information. To accomplish the security of data, all of the organization's requirements for these qualities must be met. Fulfilling only a portion of them would be insufficient. The lower section of the model displays the various security methods in an ordered manner.

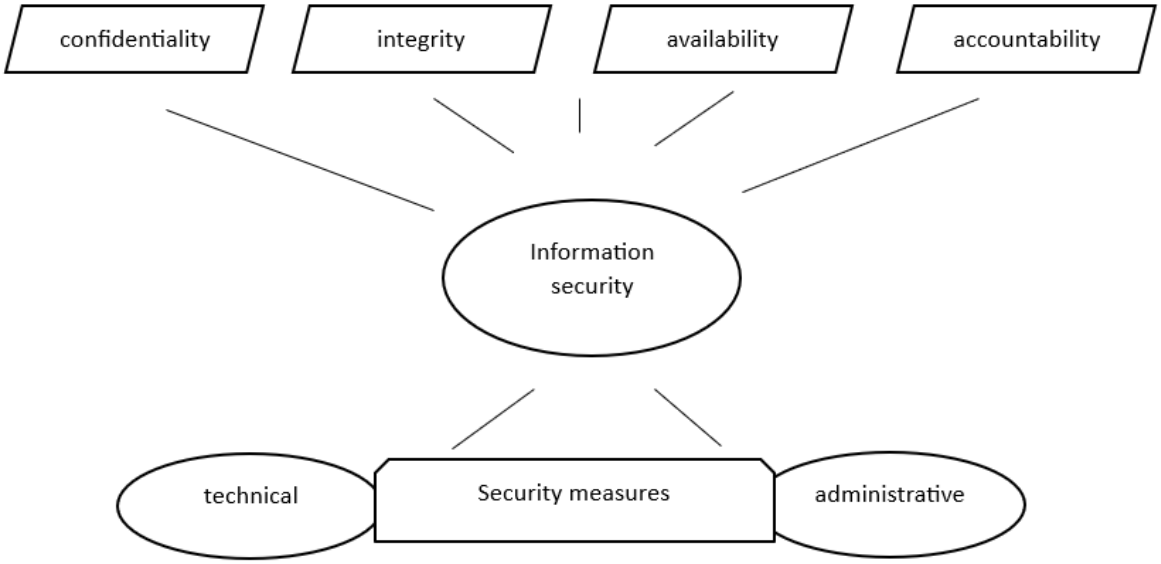

Figure 1. Information security model

The main goal of safeguarding data in higher education is to meet two critical objectives: student confidentiality and security. These phrases are well-known within the higher education sector. However, these concepts are crucial to the current study, so they have been further explained and explained. Student information is important and has to be safeguarded against misuse in order to protect students and build trust in higher education. Student safety and privacy are thus inextricably linked to student information and, by extension, the security of data. Student safety requires the correct knowledge at the right time, which includes the availability and integrity of student information. Similarly, to achieve student privacy, only the appropriate individual should have access to student information, ensuring confidentiality and responsibility. To better understand the relationship between safety and privacy regarding data security, the logic of the above was applied and integrated into the information security model (fig. 2).

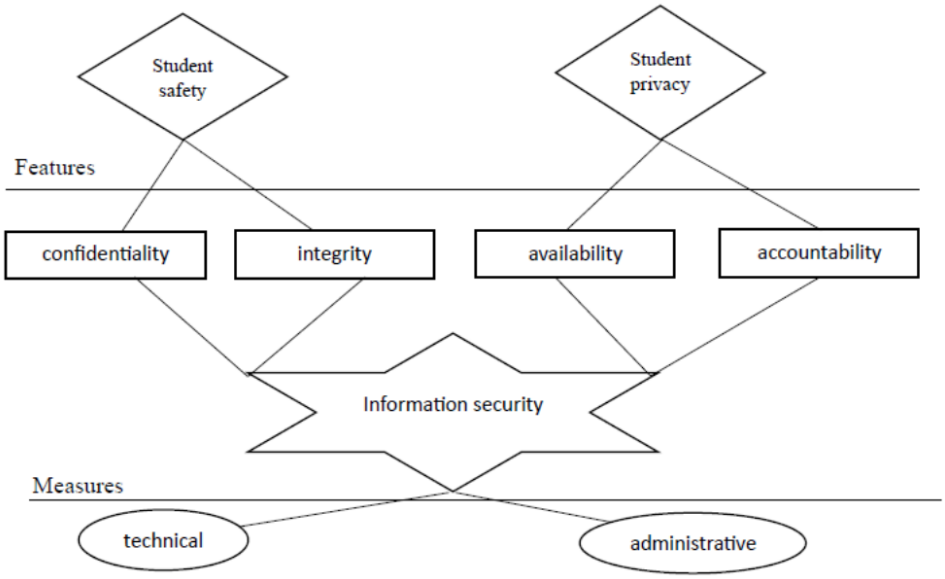

Figure 2. Model for higher education information security, adapted by (Ahlfeldt, 2008)

However, it needs to be highlighted that those connections are not unchanging, as there may be times when secrecy and transparency are required to ensure student safety, while availability and integrity are required to protect student privacy. Missing student information can jeopardize student privacy and safety, raising ethical concerns. This compromises either the student's privacy or safety. Figure 2:7 demonstrates the importance of balancing student safety and privacy in a comparable way that the information security sector has to deal with the fundamental ideas related to data security in order to reach an appropriate degree of safety for information.

CONCLUSION

The present research is an attempt to systematize the latest research findings related to the topic of information security management in higher education institutions. This research has made conceptual advances in a variety of methods by taking an analytical approach, which is based on research that used a strategy designed to improve systematicity and openness. In the first place, it has emphasized the difficulty of institutions in terms of the methods they apply when managing the security, integrity, and accessibility of the information they retain at all times. It has accomplished this by recognizing some major topics (and numerous sub-topics) covered in the literature, which include the implementation of insurance guidelines and regulations related to technology approaches to cyber-related difficulties in organizational structures executed for efficient security of data. This indicates an increasing desire and a requirement to raise the amount of research in this location; this is further demonstrated by the number of abstracts and a shortage of empirical research in the sample, as well as the fact that the majority of the articles reviewed didn't offer specific justifications for investigating information security management in colleges.

Being a late theoretical influence, the article lists themes for further research in this area, including security culture and comparisons that contrast educational institutions to other industries. Notwithstanding its mostly academic nature, a summary of research can provide useful insights, and this research is no exception. Its complete and creative technique may help both IT managers and data security teachers in schools, broadening their understanding of the present situation in managing information security work. In addition, security experts with no background in higher education may utilize the findings to obtain a grasp of the character of higher education, which includes a transparent framework, institutional structures, and a huge number of users, all of which create concerns with anonymity.

REFERENCES

1. Ahlfeldt, R-M. (2008). Information Security in Distributed Healthcare - Exploring the Needs for Achieving Patient Safety and Patient Privacy. DSV Report Series No. 08-003
2. Ahlfeldt, R-M. & Soderström E. (2007). *Information Security Problems and Needs in a Distributed Healthcare Domain – A case study*. Twelfth International Symposium on Health Information Management Research (iSHIMR 2007), Sheffield, UK, July 18 – 20, 2007, 97-108. ISBN: 0 903522 40 3.
3. Ahlfeldt, R-M., Spagnoletti, P. & Sindre, G. (2007). *Improving the Information Security Model by using TFI.* 22tn IFIP TC-11 International Information Security Conference (SEC 2007). Sandton, South Africa, May 14-16, 2007. 73-84. ISBN: 13:978-0-387- 72366-2
4. Bjorck, F. & Yngstrom, L. (2001). *IFIP World Computer Congress. IFIP TC11 WG 11.8* Second World Conference on Information Security Education, Perth, July 12-14. 209-223. Perth, Australia: International Federation for Information Processing

5. Borgman, C.L. (2018). *Open data, grey data, and stewardship: universities at the privacy frontier*. arXiv: 1802.02953
6. Chapman, J. (2019). *How safe is your data? Cyber-security in higher education. Higher Education Policy Institute,* 12. Higher Education Policy Institute, Oxford, UK, 1–6. HEPI Policy Note
7. Curry, S. (2017). *Boards should take responsibility for cybersecurity. Here's how to do it.* Harvard Business Review. Available at: https://hbr.org/2017/11/ boards- should- take- responsibility- for cybersecurity- here- how-to-do- it.
8. Dark, P. & Shanks, G., (2002). *Case Study Research, in Research methods for students, academics and professionals - Information management and systems*. Williamson K. (Ed), Second edition. Quick print
9. Doherty, N.F., Anastasakis, L., & Fulford, H. (2009). *The information security policy un- packed: a critical study of the content of university policies*. International Journal of Information Management. 29 (6), 449–457. doi: 10.1016/j.ijinfomgt.20 09.05.0 03
10. Liu, C.-W., Huang, P., & Lucas, H. (2017). *IT centralization, security outsourcing, and cybersecurity breaches: evidence from the US higher education*. International Conference on Information Systems ICIS 2017
11. Lowry, P.B., Dinev, T., & Willison, R. (2017). *Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda*. European Journal of Information Systems. 26 (6), 546–563. doi: 10.1057/s41303- 017- 0066-x
12. Okibo, B.W., & Ochiche, O.B. (2014). *Challenges facing information systems security management in higher learning Institutions: a case study of the catholic uni- versity of eastern Africa-Kenya*. International Journal of Management Excellence. 3 (1), 336–349
13. Pare, G., Tate, M., Johnstone, D., & Kitsiou, S. (2016). *Contextualizing the twin con- cepts of systematicity and transparency in information systems literature re- views*. European Journal of Information Systems. 25 (6), 493–508. doi: 10.1057/s4I303- 016- 0020- 3
14. 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*. Computer Security 66, 40–51. doi: 10.1016/j.cose.2017.01.004 .
15. Schatz, D., & Bashroush, R., (2017). *Economic valuation for information security invest- ment: a systematic literature review*. Information Systems Frontiers 19 (5), 1205–1228. doi: 10.1007/s10796-016- 9648- 8 .
16. Soomro, Z., Shah, M., & Ahmed, J. (2016). *Information security management needs more holistic approach: a literature review.* International Journal of Information Management. 36 (2), 215–225. doi: 10. 1016/j.ijinfomgt.2015.11.009 .
17. Whitson, G. (2003). *Computer security: theory, process and management*. Journal of Computing Sciences in Colleges 18 (6), 57–66.
18. Wolfswinkel, J.F., Furtmueller, E., & Wilderom, C.P.M. (2013). *Using grounded theory as a method for rigorously reviewing literature.* European Journal of Information Systems. 22 (1), 45–55. doi: 10.1057/ejis.2011.51