Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 59 – 67 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

SYSTEMIC SECURITY FRAMEWORK FOR HEI'S

Alexei Arina
Department of Software and Automation Engineering,
Technical University of Moldova

ABSTRACT: Ensuring cyber security is increasingly important for Higher Education Institutions (HEI's), the development of security frameworks based on international standards in the field, developed according to a systemic and holistic approach, has become mandatory with the digitization of the academic field and the growing number of ICT security threats. The applications used for the management of cyber security automate the entire process and enable the joint use of security requirements and the overview of the process of securing university ICT, to achieve an optimal level of cyber security of academic electronic services. In this sense, the use of European directives, security standards, and scientific methods used for the development of security frameworks, but also of formal models for the development of security systems has an important and defining role, so that the solutions developed are applicable and based on evidence scientific.

KEYWORDS*: cyber security, HEIs, management, framework, application.*

1. INTRODUCTION

The transition to the digital economy, modern health and education systems, the automation of industrial processes has favoured the development of cyber do-mains and influenced the global role they have today, to interconnect businesses and people within the global Internet communication network (Luo 2016; Huang et al. 2016).
In the new realities, where modern information technologies, IoT devices and extended Cloud services are increasingly used, ensuring cyber security is mandatory to ensure public security, business continuity and people's right to privacy in general (Asosheh, Hajinazari, and Khodkari 2013). Cyber assets have become so important that the World Economic Forum has emphasized the need to create a new class of assets, with the same importance as financial and economic assets (Merchan-Lima et al. 2020).
The purpose of scientific studies on cyber security is to provide a holistic (comprehensive) perspective, which addresses information assets through the multitude of dependencies on the technologies used, which makes the cyber security assessment process very important (Alexei 2021). The Cambridge dictionary defines the term holistic as: "that which refers to something whole or the total system, not just to its parts" (Cambridge University Press 2022).

2. THE PROBLEM OF CYBER SECURITY IN ACADEMIA

University information systems are open by design (Alexei 2021; Jang-Jaccard and Nepal 2014), decentralized, multi-user and present important platforms for study, research and university management. With the development of information and communication technologies, academic data and the communication networks used to transport them, have become important part of the university cyber domain. Thus, the digitization of universities, at the national and international levels, is required at a fast pace. The technological development of academic institutions is continuous, a strong impetus was the Covid-19 pandemic, as a result of which the entire academic activity was carried out remotely, thus increasingly using the cyber environment for online classes, access to digital courses, examination sessions, etc., which generated new conditions of activity. University campuses are becoming some of the most technologically advanced spaces.
Implementing technologies in HEIs is valuable for developing modern learning environments, but it increases the vulnerability of communication networks and the number of security threats. The multitude of technologies used creates many vulnerabilities due to the MAN (Metropolitan Area

Network) and CAN (Campus Area Network) communication networks, unlike other organizations (Joshi and Singh 2017), for example, in the banking sector.

The digitization of academic institutions highlighted the insufficiency of comprehensive studies and analyses of cyber security, becoming over time an important problem for the educational field (Fouad 2021), requiring multiple scientific studies on this dimension. The interest of cyber attackers is diverse: the theft of intellectual property, which refers to the results of research carried out by HEIs, often for organizations that are part of the Critical State Infrastructure, which have much more secure systems, and to university systems attackers can gain access much easier; significant financial losses or interruption of electronic academic services, unavailability of electronic communication networks.

In the annual reports published by Microsoft and Check Point Software (Check Point Research 2022), the multinational provider of solutions for securing organizations, the most targeted industries in 2022 were the education and research sector, the ICT (Information and Communication Technology) sector and non-governmental organizations (Figure 1).

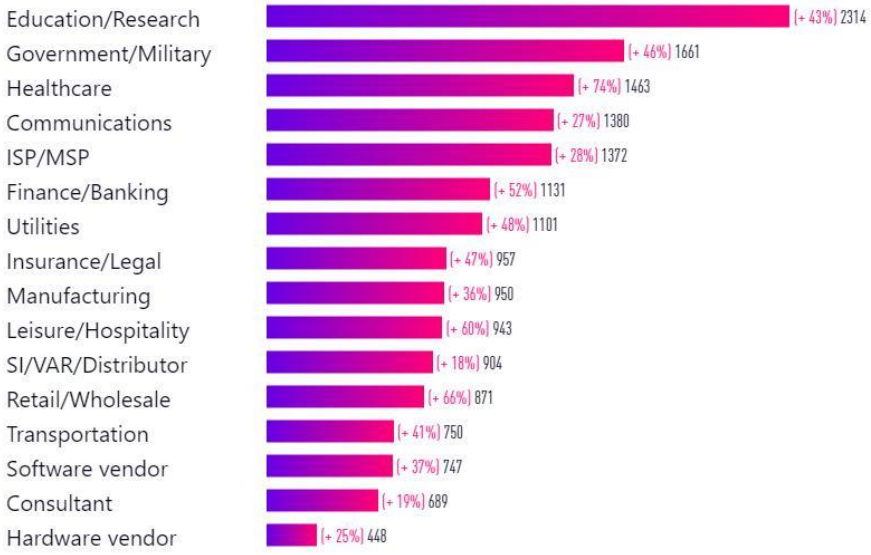

Fig.1. *The number of weekly security attacks reported in 2022, compared to 2021 (Check Point Research 2022)*

Also, as can be seen in Figure 2, according to the Microsoft Digital Defense Report (Microsoft 2023) published in October 2023, the education sector remains the most targeted by cyber attackers.

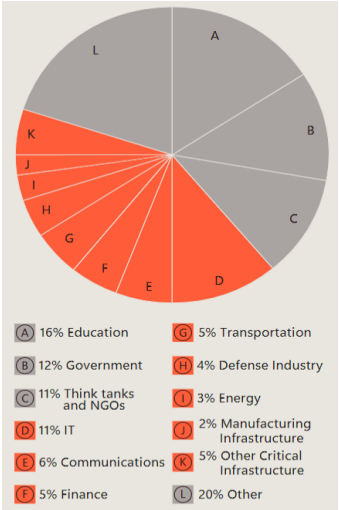

Fig.2. *Most targeted sectors globally (Microsoft 2023)*

Although the educational field witnesses a continuous annual increase in the number of cyber-attacks, few studies focused on the implementation of holistic security frameworks in HEIs have been identified in the specialized literature (Fouad 2021), (Rehman, Masood, and Cheema 2013), compared to other banking (Panja et al. 2013), medical (Coventry and Branley 2018) or industrial fields (Ani, He, and Tiwari 2019). None of the three dimensions with major social impact, described previously, affect any criterion of existentialism (Fouad 2021).

The need for a holistic approach to cyber security in HEIs is increasingly highlighted, in order to ensure the achievement of educational processes, the security of university data and financial resources, to add value to the development of the theoretical and practical bases of the cyber security field. The development of an application that allows the implementation of common security requirements for HEIs would respond to the European normative frameworks, which through the NIS_2 Directive (European Parliament 2022), require the implementation of common security requirements for the same fields. Thus, in the following sections, the security framework developed for HEIs and the prototype of an application will be presented that will allow to joint use of the security requirements for HEIs from the Republic of Moldova.

3. CYBERSECURITY FRAMEWORK

The security framework was developed using the Security Requirements Engineering SRE scientific method (Mellado, Fernández-Medina, and Piattini 2006). The development of the security framework was presented in a previously published paper (Alexei Ar., Nistiriuc P., and Alexei An., 2022) and includes:" development of security policies, identification of important informational assets, identification of security objectives and system dependency, identification of security threats, cyber risk assessment, identification of security requirements, completing the repository with relevant security controls" (Alexei Ar., Nistiriuc P., and Alexei An., 2022).

The graphical representation in Figure 3 of the operational security framework enables the analysis of the entire research rationale and the essential elements of the proposed security framework.

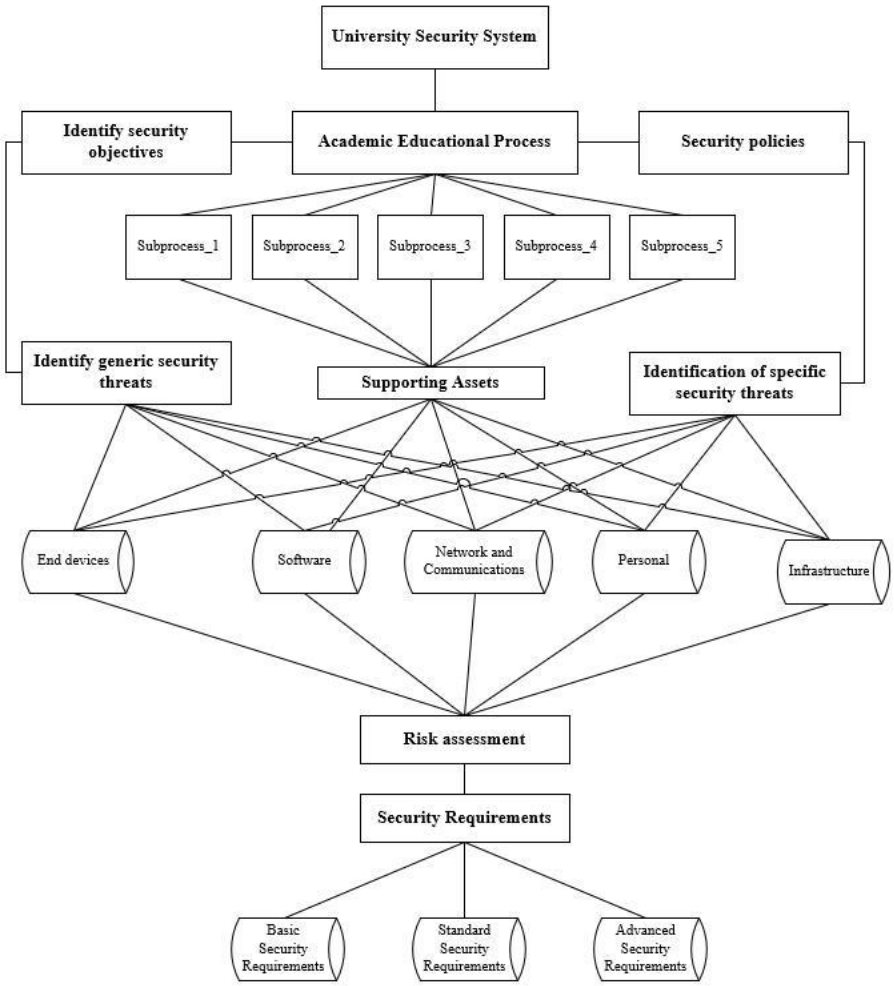

Fig.3. *University Operational Security Framework*
(Alexei Ar., Nistiriuc P., and Alexei An., 2022)

The operational security framework will be able to be evaluated in terms of the identified Key Performance Indicators (KPIs), for each of the 7 stages. Performance indicators are used to measure the level of security within organizations (Bolun 2021), concerning a specific control point, to provide evidence for effective administration: technical and managerial (Alexei Ar., Nistiriuc P., and Alexei An., 2022).

Performance indicators can serve as tools used for decision-making (Wang 2005) and for setting measurable objectives (Bolun 2021). The key indicators of the proposed security framework have been identified according to the operationalization stages and represent the finality of each stage, as reflected in Figure 4.

The performance indicators were selected according to the provisions of inter-national standards, such as ISO 27001 (ISO/IEC 2023) and ISO 27005 (ISO/IEC 27005 2018), of the European regulatory framework the NIS_2 directive (European Parliament 2022), based on the Clements-Hoffman security model (Lance J. Hoffman and Don Clements 1977).

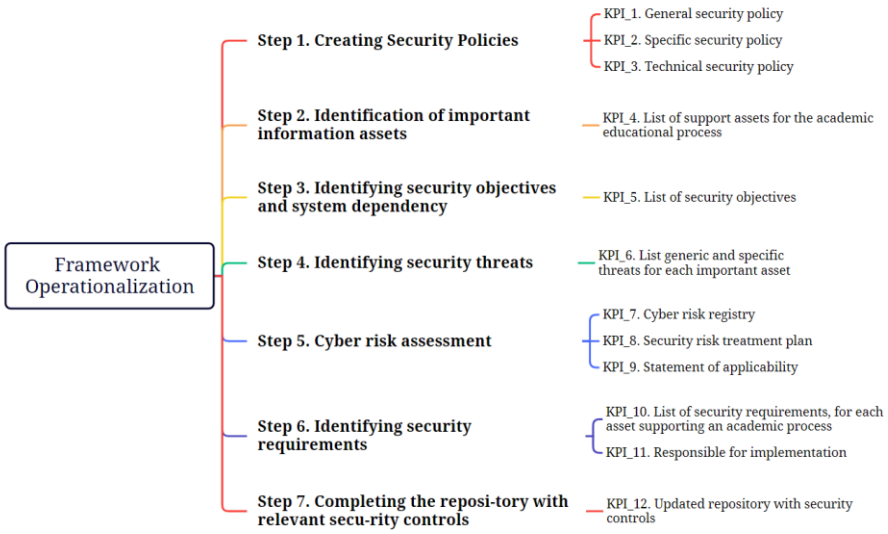

Fig. 4. *Framework implementation stages and KPIs (Alexei Ar., Nistiriuc P., and Alexei An., 2022)*

The goal of security is subjective, while performance indicators are objective and allow the evaluation of a certain security framework by experts or audit teams. Thus, indicators related to security policies are important to ensure that users comply with the provisions of the security framework, so the intention to implement a security framework must be supported by specific documents, administrative security policies and system-based policies (technical). In the case of administrative security policies, information through periodically revised documents, depending on the changes made in the university ICT systems, can ensure the compliance of the user's actions of the ICT system with the security requirements of the framework. System-based security policies are the configurations of ICT technologies through which access to university ICT can be controlled.

According to the Clements-Hoffman model, assets represent the reference point of security systems, so generating the list of supporting assets will allow an overview of the components of university ICT systems that require security.

Security objectives represent the fundamental principles of cyber security, determining the relationship between the security objective and the primary university asset, contributes to the correct and reasoned determination of security requirements. Therefore, if availability is critical for a particular asset, then the security requirements implemented must prioritize preventing/correcting problems related to the availability of university academic services.

Security threats are fuzzy sets of data, but to achieve an optimal security scenario, it is necessary to determine a defined set of generic and specific threats, as an essential part of the security system, to know the spectrum of existing threats, and along the way this the list must be updated periodically as new threats risk exploiting university ICT assets, which will enable the implementation of security control 5.7. Threat intelligence, of the ISO 27001 standard (ISO/IEC 2023).

According to the ISO 27005 standard (ISO/IEC 27005: 2018), any organization that implements security systems must perform a cyber risk assessment to identify the risks associated with the use of ICT technologies, thus increasing the effectiveness of these systems. In this sense, the risk register will allow centralized management for the analysis of existing risks in ICT systems. Based on the risk management plan, the managers will make decisions regarding the risks that can be ignored or treated.

Security requirements are the building blocks of a security system, according to the Clements-Hoffman model (Lance J. Hoffman and Don Clements 1977). Their identification will allow them to secure the vulnerable access paths to the ICT systems and the implementation of the common requirements for academia. To control the process of implementing the security requirements, responsible persons must be appointed. The Statement of applicability is a mandatory document, which must be completed by any university that intends to be certified with the ISO 27001 standard. In the declaration, the implemented security requirements are argued and objective justifications are provided in the case of certain ISO 27001 (ISO/IEC 2023) requirements that are not relevant to the HEIs.

The indicator that refers to the updated repository with security controls will be able to be used to implement the common security requirements, according to the provisions of the NIS2 directive (European Parliament 2022). Moreover, it will allow mandatory security checks to be performed, such as 5.27. Learning from security incidents and 5.28. Collection of evidence, of the ISO 27001 standard (ISO/IEC 2023).

4. DEVELOP A SECURITY FRAMEWORK APPLICATION PROTOTYPE

The previous section presented the implementation steps and key activities of the security framework. To ensure the unification of efforts in the implementation of the security framework, an application prototype (i-CSSCE) was developed that will allow the selection of the performance indicators for each stage. Finally, a report is generated that can be used to evaluate the level of implementation of the security framework and to observe the indicators that have not yet been satisfied, for decision-making. The tool could be used simultaneously by several users and HEIs, allows the creation of several projects, presents itself as a management platform for academic electronic services, which allows the management of organizational and operational aspects of the security framework, by identifying important information assets, identifying security threats, security requirements and controls that have been or are needed to be implemented to make informed decisions.

The i-CSSCE tool can support the implementation process of the activities proposed by the security framework, to minimize the effort required for information security management activities. It was designed as a web application written in PHP, HTML5, and JavaScript and uses MySQL databases. Client-side viewing takes place in the browser and will be able to run on any system that supports PHP, JavaScript, and MySQL. The tool consists of several separate modules, which will be usable depending on the user's access rights. The user interface of the application consists of several related web pages, which can be accessed from the menu, each page is associated with certain specific activities and interacts with each other through a MySQL-based database.

According to the Clements-Hoffman formal model, which describes the primary components of a security system, functions were created that will later allow management the relationships between them, the EER diagram reflecting the relationships between the elements of the security framework can be analysed in the figure 5.

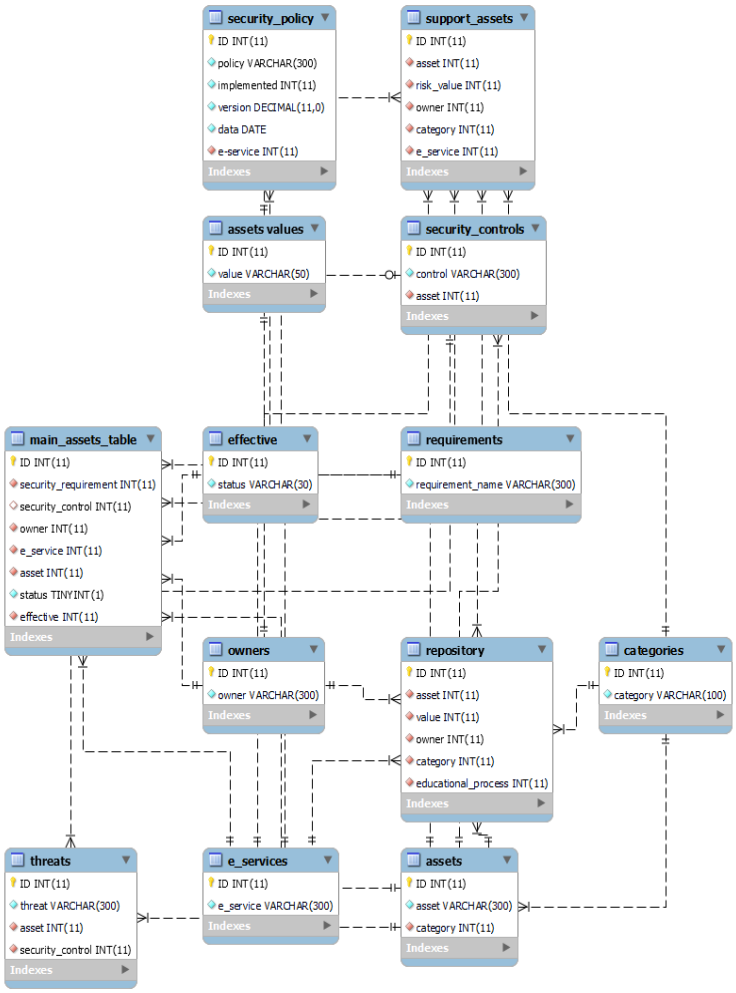

Fig.5. *The relationships between the elements of i-CSSCE*

The i-CSSCE tool allows management and assess the level of implementation of the operational security framework.

5. CONCLUSION

The basic objective of i-CSSCE consists of determining the necessary actions for the implementation of a complete security system framework and the implementation of common security requirements for the educational field, which is one of the European priorities, according to the provisions of the European NIS_2 Directive. The i-CSSCE prototype could be used as a guide in the process of implementing the security framework and to have an overview of the status of ICT security in HEIs.

The holistic approach to cyber security in HEIs is increasingly important, because as described in the introduction of this article, the educational field, especially HEIs is one of the most targeted fields in 2023, so the systemic and comprehensive approach becomes mandatory for the academia.

The development of the security framework and application prototype according to the Clements-Hoffman model, which establishes the relationships between the elements of the security systems, will allow us to systematically and holistically approach cyber security in HEIs.

REFERENCES

1. Alexei, Arina. 2021. “Network Security Threats to Higher Education Institutions.” In *CEE E|Dem and E|Gov Days*, 32333. Budapest. https://doi.org/10.24989/ocg.v341.24.
2. Alexei Ar., Nistiriuc P., and Alexei An. 2022. “The Holistic Approach to Cybersecurity in Academia.” In *CEEeGov '22: Proceedings of the Central and Eastern European eDem and eGov Days*, edited by NY, USA ACM. New York. DOI: https://doi.org/10.1145/3551504.3551516.
3. Ani, Uchenna Daniel, Hongmei He, and Ashutosh Tiwari. 2019. “Human Factor Security: Evaluating the Cybersecurity Capacity of the Industrial Workforce.” *Journal of Systems and Information Technology* 21 (1): 2–35. https://doi.org/10.1108/JSIT-02-2018-0028.
4. Asosheh, Abbass, Parvaneh Hajinazari, and Hourieh Khodkari. 2013. “A Practical Implementation of ISMS.” In *7th International Conference on E-Commerce in Developing Countries:With Focus on e-Security*. IEEE. https://doi.org/10.1109/ECDC.2013.6556730.
5. Bolun, I. 2021. “Prioritization of Cybersecurity Measures.” In *The 11th International Conference OnElectronics, Communications and Computing*, 194–99. Chișinău.
6. Cambridge University Press. 2022. “Cambridge Academic Content Dictionary.” 2022. https://dictionary.cambridge.org.
7. Check Point Research. 2022. “Cyber Security Report.” https://www.checkpoint.com.
8. Coventry, Lynne, and Dawn Branley. 2018. “Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward.” *Maturitas* 113 (July):48–52. https://doi.org/10.1016/j.maturitas.2018.04.008.
9. European Parliament, Council of the European Union. 2022. “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive).”
10. Fouad, Noran Shafik. 2021. “Securing Higher Education against Cyberthreats: From an Institutional Risk to a National Policy Challenge.” *Journal of Cyber Policy* 6 (2): 137–54. https://doi.org/10.1080/23738871.2021.1973526.
11. Huang, X., P. Craig, H. Lin, and Z Yan. 2016. “SecIoT: A Security Framework for the Internet of Things.” *Security and Communication Networks* 9 (16): 3083–94.
12. ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT. International Organization for Standardization. Geneva, Switzerland, 2022.
13. ISO/IEC 27005: Information technology – Security techniques – Information security risk management. International Organization for Standardization. Geneva, Switzerland, 2018.
14. Jang-Jaccard, Julian, and Surya Nepal. 2014. “A Survey of Emerging Threats in Cybersecurity.” In *Journal of Computer and System Sciences*, 80:973–93. Academic Press Inc. https://doi.org/10.1016/j.jcss.2014.02.005.
15. Joshi, Chanchala, and Umesh Kumar Singh. 2017. “Information Security Risks Management Framework – A Step towards Mitigating Security Risks in University Network.” *Journal of Information Security and Applications* 35 (August). https://doi.org/10.1016/j.jisa.2017.06.006.
16. Lance J. Hoffman, and Don Clements. 1977. “FUZZY COMPUTER SECURITY METRICS: A PRELIMINARY REPORT.” Berkeley.
17. Luo, X. 2016. “Security Protection to Industrial Control System Based on Defense-in- Depth Strategy.” *WIT Transactions on Engineering Sciences* 113:19–27.
18. Mellado, Daniel, Eduardo Fernández-Medina, and Mario Piattini. 2006. “Applying a Security Requirements Engineering Process.” In , 192–206. https://doi.org/10.1007/11863908_13.
19. Merchan-Lima, Jorge, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez-Fonseca, and Dorys Quiroz. 2020. “Information Security Management Frameworks and Strategies in Higher Education Institutions: A Systematic Review.” *Annals of Telecommunications*, July. https://doi.org/10.1007/s12243-020-00783-2.
20. Microsoft. 2023. “Microsoft Digital Defense Report.”
21. Panja, Biswajit, Dennis Fattaleh, Mark Mercado, Adam Robinson, and Priyanka Meharia. 2013. “Cybersecurity in Banking and Financial Sector: Security Analysis of a Mobile Banking

Application." In *2013 International Conference on Collaboration Technologies and Systems (CTS)*, 397–403. IEEE. https://doi.org/10.1109/CTS.2013.6567261.

22. Rehman, Huma, Ashraf Masood, and Ahmad Raza Cheema. 2013. "Information Security Management in Academic Institutes of Pakistan." In *2013 2nd National Conference on Information Assurance (NCIA)*. IEEE. https://doi.org/10.1109/NCIA.2013.6725323.
23. Wang, Andy Ju An. 2005. "Information Security Models and Metrics." In *Proceedings of the 43rd Annual Southeast Regional Conference on - ACM-SE 43*, 178. New York, New York, USA: ACM Press. https://doi.org/10.1145/1167253.1167295.