Intelligent Human Systems Integration (IHSI 2025), Vol. 160, 2025, 223–233
https://doi.org/10.54941/ahfe1005828

Exploring Cybersecurity Challenges of Digital Transformation in Higher Education

Fatimah Alshahrani, Shouq Alyami, Mahdi Alyami, and Abdulmajeed Alqhatani

Department of Information Systems, College of Computer Science & Information Systems, Najran University, Najran 61441, Saudi Arabia

ABSTRACT

Cybersecurity is a critical issue when it comes to the digital transformation of operations and services undertaken by many organizations and sectors worldwide. In Saudi Arabia, the government aimed to improve the education sector by integrating the latest technologies in learning and by automating the workflow within schools and universities. In this study, we explore how potential cybersecurity threats resulting from the digital transformation are managed by Saudi higher educational Institutions. We conducted semi-structured interviews with cybersecurity and digital transformation experts to understand their digital transformation and risk management plans and practices. Based on our findings, the adoption of advanced technologies, such as IoT devices and cloud computing services, can lead to security and privacy risks, particularly the possibility of unauthorized access and misuse of data. Our study also reveals the key challenges organizations face when securing their systems, including the limited awareness among staff and students about cybersecurity issues and data compliance rules, the lack of resources, and the legacy systems and infrastructures. This study also outlines a set of practices to protect the digital infrastructure and resources within educational institutions.

Keywords: Digital transformation, Information technology, Cybersecurity, Education

INTRODUCTION

In this era of rapid technological advancements, Information Technology (IT) plays a salient role in improving the quality of operations and services in organizations. IT has dramatically increases the chances for innovation and efficiency across different domains, enabling organizations to automate workflows, improve performance, and enhance productivity.

In the higher education domain, the ongoing scientific and technological revolution has altered the way of delivering the learning and training to students. This transformation is driven by an increasing dependence on information and communication technologies, which has led to the emergence of new pedagogical paradigms (e.g., virtual and smart learning). As a result, educational institutions are forced to adapt to this digital shift by building robust digital infrastructures capable of competing within the ever-expanding cyberspace. This adaptation requires a well-developed digital transformation plan that includes rich information systems, cloud computing, Internet of Things (IoT), and mobile communications to ensure comprehensive benefits (Akour and Alenezi, 2022).

However, digitizing services can also introduce serious security and privacy risks, which imposes challenges on any digital transformation efforts. Previous studies indicate that educational institutions are particularly vulnerable to cyberattacks due to managing large amounts of information, which require robust cybersecurity measures (Ulven and Wangen, 2021). As educational institutions continue to embrace digital transformation, they must understand and mitigate the cybersecurity risks associated with these developments.

In this study, we examine cybersecurity challenges related to the digital transformation within Saudi higher education institutions. We focus on Saudi institutions because the government has focused heavily on introducing the latest digital technologies into education as part of the vision 2030 that seeks to accelerate the digital transformation of services (Saudi Vision, 2030). Overall, this research has three main objectives:

- To explore the digital transformation effort undertaken by Saudi higher educational institutions.
- To understand how digital transformation within education could impact cybersecurity
- To investigate the current practices and challenges in protecting information and the digital infrastructure against cybersecurity threats

BACKGROUND

Digital Transformation

There are several definitions of digital transformation in the relevant literature. Digital transformation refers to the ongoing cultural, organizational, and operational changes that occur within an organization, industry, or ecosystem as a result of the intelligent integration of digital technologies, processes, and capabilities at all levels and functions (Saarikko et al., 2020). This transformation impacts people, processes, strategies, structures, and competitive dynamics, demanding substantial organizational changes due to the technology integration (Serna Gómez et al., 2021; Alenezi, 2021). Digital transformation is the strategic and prioritized evolution of business and organizational operations, processes, capabilities, and models to fully leverage the opportunities presented by a combination of digital technologies and their broader societal impact (Serna Gómez et al., 2021).

Previous studies have investigated digital transformation in the education sector. The study conducted by Benavides et al. (2020) indicates that digital transformation in higher education institutions encompasses various dimensions, including infrastructure, curricula, management, financial and technological aspects, research, human resources, guidance, governance, information, marketing, and business operations. Fernández et al. (2023) examined digital transformation initiatives at higher education institutions, emphasizing the quality and competitive education. Their study demonstrates that advanced analytics, cloud computing, and artificial intelligence are the most frequently utilized technologies. Therefore, educational institutions can take advantage of the modern technologies and breakthroughs in artificial intelligence. Universities are adapting to digital transformation by implementing contemporary technologies (e.g., blockchain, artificial intelligence and chatbots) to enhance efficiency and to adapt to the changing environment (Tamer and Knidiri, 2023).

However, several challenges may hinder digital transformation within the education domain. Gkrimpizi et al. (2023) identified several issues, including a lack of digital knowledge, apprehension about change and risk, insufficient IT infrastructure, budgetary constraints, inadequate change leadership, insufficient strategic planning, and concerns about security and privacy. Rodríguez and Bribiesca (2021) also reported ineffective leadership, cultural resistance, and lack of financial support as barriers to the adoption of digital transformation. García (2021) emphasized that institutional strategies and policies must be strengthened to facilitate the digital transformation of higher education institutions. Yet, concerns about security and privacy can deter higher education institutions from adopting digital technologies (Gkrimpizi et al., 2023), which we will discuss in the next subsection.

The Impact of Digital Transformation on Cybersecurity

The use of digital technologies has increased security and privacy risks. A common concern is the risk of data breaches, which can lead to the exposure of sensitive information (Ulven and Wangen, 2021). Moreover, in the context of digital transformation, many institutions rely on third-party vendors to digitize their services, aiming to enhance flexibility and scalability. While this outsourcing can offer many advantages, it also brings potential risks, such as compliance with regulations, unauthorized access to data, and service disruption issues (Serna Gómez et al., 2021).

Higher education institutions are particularly vulnerable to security threats due to the large volume of information they store and process, such as student records (Ulven and Wangen, 2021). Security attacks, such as data breaches, can disrupt academic and administrative processes, affecting students, instructors, and staff (Garba et al., 2020). The consequences of security attacks may also damage the reputation of academic institutions and may result in financial losses (Li and Liu, 2021). Gebremeskel (2023) identified several information security challenges by organizations undergoing digital transformation, which include security breaches and limited access to and control over information.

Therefore, organizations should have a well-established cybersecurity plan to deal with the associated risks of digital transformation (Saeed et al., 2023). This plan should take into account the importance of awareness in fostering a secure digital environment (Alhalafi and Veeraraghavan, 2023). Furthermore, digital risks can be mitigated with clear security policies and robust technological defenses (Omar, 2020; Shah, 2022). In this study, we investigate the practices of educational institutions aimed to protect the security of their digital systems.

METHODOLOGY

In this section, we describe our study method, procedure, and data analysis approach. This study was approved by our university Research Ethics Committee.

Interview Study

We conducted 12 semi-structured interviews with digital transformation and cybersecurity experts from four government higher educational institutions in Saudi Arabia. Through the interviews, we sought to understand digital transformation initiatives within higher educational institutions, how this transformation affected the security and privacy of resources, and what actions and practices these institutions took to protect their resources. The experts were recruited through personal contacts and snowball sampling. While six interviews were conducted in person, the other six were carried out through phone and video conferencing. Interviews ranged from 17–60 minutes long and lasted an average of 30 minutes. The interview was audio-recorded if the participant consented, and we transcribed all recordings for data analysis. Table 1 summarizes the participants' information.

Table 1. Summary of participants information.

Expert	Age, Gender	Education Level	Position	Years of experience
E1	43, M	Doctorate	HoD of digital transformation	4
E2	38, M	Doctorate	Vice deanship of digital transformation	5
E3	37, F	Doctorate	Digital transformation consultant	6
E4	46, M	Bachelor	IT manager	12
E5	34, M	Master	Cybersecurity assistant manager	4
E6	34, M	Master	Cybersecurity manager	5
E7	41, M	Doctorate	IT governance and digital transformation consultant	4
E8	25, F	Bachelor	Administrative assistant in the digital transformation department	3
E9	40, M	Doctorate	Digital transformation consultant	6
E10	34, M	Master	Administrative assistant in the digital transformation department	5
E11	40, M	Bachelor	IT specialist	11
E12	37, M	Doctorate	Digital transformation consultant	4

Procedure

The interview questions were semi-structured, with some questions asked depending on the context of the conversation. The interviews began by asking participants about the digital transformation effort in their respective organizations. For example, participants were asked what services are being digitalized, what specific hardware and software are needed, and how the digitalization of services is implemented. We also asked the participants how the digital transformation affects the organizations' services and operations. The second part of the interview then focused on the security and privacy threats that can result from a digital transformation. For instance, we asked whether any digital services can be vulnerable to specific attacks. The questions also addressed not only the plans and actions to secure resources, but also the challenges faced by organizations to protect those resources. Finally, we collected some demographic information from the experts.

Data Analysis

We used thematic analysis to identify patterns from the interviewees' responses. First, two members of the research team independently coded three interview scripts to create codes. The two researchers then met to discuss their codes, resolve their disagreements about the different codes, and create a unified codebook. The researchers then coded the remaining transcripts using the codebook. The resulting inter-rater agreement is 88%. We used the QDA Miner Lite software to analyze data and to create codes. The resulting codes falls under three broad categories: digital transformation, security and privacy issues, and protection methods. The identified patterns and data helped us understand the most perceived cybersecurity threats when undergoing digital transformation in higher education and the common challenges when protecting digital resources. In the next section, we discuss the detailed results.

RESULTS

First, we discuss our experts' views and practices about the digital transformation in their organizations. Then we explain the security and privacy issues related to digital transformation. We conclude this section by listing a set of practices that help protect digital resources against cyber-threats.

Digital Transformation in Higher Education Institutions

In general, the experts held a shared conception and views about the goal of digital transformation in higher education. The experts described digital transformation as the integration of digital technologies into all academic and administrative aspects to automate operations and services. E9 stated: *"The main goal of digital transformation is the migration from traditional paper-based systems to digital solutions, while providing digital services and 24-hour access to the information, it also aims to enhance communication* *efficiency and develop information systems that meet business and user needs.”*

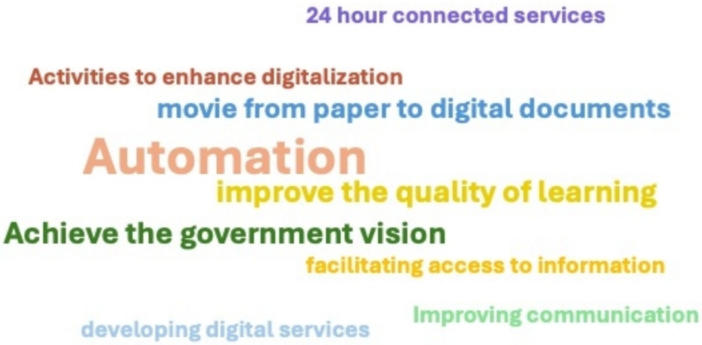
24 hour connected services
Activities to enhance digitalization
movie from paper to digital documents
Automation
improve the quality of learning
Achieve the government vision
facilitating access to information
Improving communication
developing digital services

Figure 1: The most common objectives of digital transformation.

The Digital Government Authority (DGA) is responsible for not only tracking and measuring the performance of government agencies, including the academic sector, in relation to digital services, but also ensuring that agencies provide high-quality digital services to the beneficiaries. Therefore, the strategic directions of higher educational institutions should align with those of the DGA, which should be aligned with the strategic directions of the Saudi government’s vision. E1 stated, “*The university has a strategic plan for digital transformation derived from the general strategy of the National Authority for Digital Transformation, which must be followed by all government entities.*” In addition, the strategy should consider the engagement and collaboration of all stakeholders, including students, staff, and external parties.

We also asked the experts about the tools and technologies used for implementing a digital transformation. Our experts reported a wide range of resources used to expediate the workflow, manage the operations in different workplace settings, and enhance the quality of the learning environment. These resources include core digital infrastructure (high-speed internet, networking, data centers, servers, backup drives), learning support tools (learning management system, e-mail service, academic advising portal, research management system), operation support systems (customer relationship management, enterprise resource planning, electronic correspondence system), and data and security management systems (firewall, intrusion detection and prevention systems). In addition, these resources should be complemented with 24-hour maintenance and continuous improvements.

Security and Privacy Threats and Challenges

The histogram in Figure 2 below shows the most common challenges encountered by the examined institutions in implementing digital transformation. As the figure shows, security was listed as the most challenging aspect, with additional aspects related to security and privacy (e.g., third-party risk and data privacy compliance) also being listed by the experts. Due to storing a significant amount of sensitive data, including personal information of students and staff, financial and academic records, and research data, universities can be targeted by cyber attacks. E6 indicated that technologies, such as a cloud computing service, increase the accessibility and mobility of data, which can increase the risk of unauthorized access. The use of modern technologies, such IoT devices that collect a massive amount of data, poses additional security challenges. Three participants stated that the risk may also come from inside users, such as students and staff, who might intentionally or unintentionally misuse the resources.

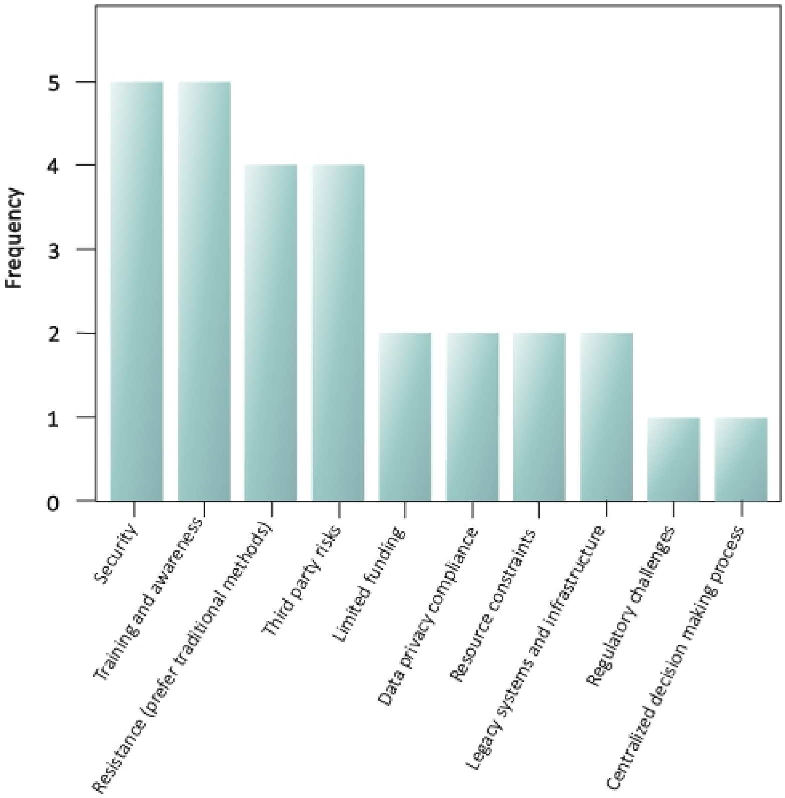

Figure 2: Digital transformation challenges in higher educational institutions in Saudi Arabia.

In this regard, many of our study experts indicated a lack of awareness exists among students and staff regarding the potential security and privacy threats and the proper security practices. This limited awareness makes individuals an important target by cyber attacks. E4 pointed out that *"if people are unaware of the potential security risks, our digital resources will be at risk. Awareness is a fundamental pillar in the digital transformation process."*

Academic institutions must ensure that their digital transformations adhere to all applicable legal standards and regulations, such as the Saudi

Personal Data Protection Law (PDPL). These regulations impose strict rules on how organizations can handle personal data. The adherence to these regulations extends to all members of the organization, such as students and staff, when using the institution's resources. However, E2 also noted that students may be unaware of the policies concerning the use of digital systems, which imposes another challenge. "*Students are generally less aware about security rules. One day we received an alert from the system about a suspicious activity: two access to the system from two different geographical locations at the same time by the same user's credential. And that actually occurred because the student shares his login information with his friend*".

Finally, building trust with customers through robust cybersecurity systems can enhance the institution credibility within the education sector. The experts linked the aspect of trust with the integration of the latest security systems. Yet, institutions might be challenged with legacy systems. At the same time, a few experts in our study also indicated being hindered by limited financial support to incorporate the most advanced security tools in the workplace.

Protective Measures

In this part of the results, we identify a set of measures that our experts reported undertaking or suggested for enhancing the security and privacy of digital resources. These protective measures include traditional and technical-based methods.

Classifying data and their security level. This process helps organizations to prioritize data based on their sensitivity, and thus implements the appropriate level of protection for each type of data. In addition, organizations should provide clear guidelines to all members within the organization on how to use data and other resources.

Implementing advanced communication and monitoring tools. These tools can help in the early detection of security incidents, allowing for immediate response to mitigate the impact of any attack. Such tools, as mentioned by our experts, include advanced firewalls combined with intrusion detection systems, encryption and secure channels to protect the connection and transfer of data.

Backing up and recovering data. Organizations must maintain a reliable data backup is in case of system failures or data losses. Backups should be periodically tested and automatically performed through software or a cloud storage service.

Implementing strong access control and authorization. System and security admins within organizations can perform specific steps to enhance the access control system security. For example, enforcing strong authentication methods (e.g., 2-factor authentication) and using secure access control models (e.g., role-based access control) can prevent access to resources by unauthorized users. Another good practice is having security audit personnel to review permissions and avoid unauthorized access. Principles, such as the least privilege principle, can also ensure the access to data and resources by users is limited to only performing their tasks.

Educating and raising awareness. This important aspect was mentioned by most participants. As digital transformation involves the use of advanced technologies, new security challenges can arise, which requires an affective awareness program to educate staff and students about the emerging risks and how to manage personal and institutional security and privacy. Educating members can be as simple as encouraging them not to share their login credentials with others and using strong passwords, or by conducting a simulated phishing attack and social engineering training.

Performing regular software updates. Updates are an important security practice because unpatched software can lead to system vulnerabilities that can be exploited by hackers. Updating software provides several advantages, including fixing bugs, adding new software features and functionalities, and ensuring compatibility with the new systems.

Preparing a disaster recovery plan. Academic institutions should have a comprehensive recovery plan in the form of a document that describes how to deal with and respond to accidental system failures or malicious attacks. Institutions should also designate a team of experts and train them adequately and regularly, providing those trained with the necessary tools to handle different incidents.

DISCUSSION AND CONCLUSION

The findings from this study provide insight into the challenges faced by higher education institutions regarding digital transformation. Our study experts listed several factors that may hinder digital transformation efforts within their institutions, with security being considered the most challenging aspect. Our study also reveals a set of actions taken to safeguard digital resources against cyber threats.

Digital transformation involves the integration of digital technologies into nearly all aspects of an institution's services and operations. This study asserts that academic institutions should partner with government and private sectors to exchange information and expertise regarding potential threats and the most effective defenses against these threats in order to achieve successful digitalization. Additionally, collaboration among universities is essential, as they are likely to face similar attack techniques targeting their systems. Organizations should invest in the latest security solutions to counter evolving cyber threats and enhance their cyber resilience. This investment must be accompanied by continuous monitoring, regular updates, and the development of response protocols, which are essential components of a robust cybersecurity strategy that supports broader digital transformation goals.

The human factor cannot be overlooked when addressing the security and privacy aspects of digital systems. In fact, our study experts were significantly concerned about the lack of cybersecurity knowledge among members in their workplace environment. Thus, academic institutions should develop training and awareness programs in order to help their members understand potential security risks and enable them to navigate digital platforms securely and effectively. In addition, Saudi higher education institutions should educate their members on the safe use of digital resources, which must be in accordance with the regulations of the DGA and other applicable regulations.

In conclusion, our study presents the perspectives of 12 experts on digital transformation and the related security and privacy risks in higher education. While many institutions are striving to digitalize their operations and services to improve their working and learning environments and align with the Saudi government's vision, several factors can hinder this digitalization. Among these factors are security, legacy systems, and a lack of awareness and financial resources. Future studies are recommended to develop a comprehensive framework of the factors influencing digital transformation in higher education.

REFERENCES

Akour, M. and Alenezi, M., 2022. Higher education future in the era of digital transformation. *Education Sciences*, *12*(11), p. 784.

Alenezi, M., 2021. Deep dive into digital transformation in higher education institutions. *Education Sciences*, *11*(12), p. 770.

Alhalafi, N. and Veeraraghavan, P., 2023. Exploring the challenges and issues in adopting Cybersecurity in Saudi Smart cities: Conceptualization of the Cybersecurity-based UTAUT Model. *Smart Cities*, *6*(3), pp. 1523–1544.

Benavides, L. M. C., Tamayo Arias, J. A., Arango Serna, M. D., Branch Bedoya, J. W. and Burgos, D., 2020. Digital transformation in higher education institutions: A systematic literature review. *Sensors*, *20*(11), p. 3291.

Fernández, A., Gómez, B., Binjaku, K. and Meçe, E. K., 2023. Digital transformation initiatives in higher education institutions: A multivocal literature review. *Education and information technologies*, *28*(10), pp. 12351–12382.

Garba, A., Sirat, M. B., Hajar, S. and Dauda, I. B., 2020. Cyber security awareness among university students: A case study. *Science Proceedings Series*, *2*(1), pp. 82–86.

García-Peñalvo, F. J., 2021. Avoiding the dark side of digital transformation in teaching. An institutional reference framework for eLearning in higher education. *Sustainability*, *13*(4), p. 2023.

Gebremeskel, B. K., Jonathan, G. M. and Yalew, S. D., 2023. Information security challenges during digital transformation. *Procedia Computer Science*, *219*, pp. 44–51.

Gkrimpizi, T., Peristeras, V. and Magnisalis, I., 2023. Classification of barriers to digital transformation in higher education institutions: Systematic literature review. *Education Sciences*, *13*(7), p. 746.

Li, Y. and Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, pp. 8176–8186.

Omar, A., 2020. Towards an integrated model of data governance and integration for the implementation of digital transformation processes in the Saudi universities. *International Journal of Advanced Computer Science and Applications*, *11*(8).

Rodríguez-Abitia, G. and Bribiesca-Correa, G., 2021. Assessing digital transformation in universities. *Future Internet*, *13*(2), p. 52.

Saarikko, T., Westergren, U. H. and Blomquist, T., 2020. Digital transformation: Five recommendations for the digitally conscious firm. *Business horizons*, *63*(6), pp. 825–839.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E. and Alabbad, D. A., 2023. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), p. 6666.

Saudi Vision 2030. *"https://www.vision2030.gov.sa/en"* [Accessed online: November 3, 2024].

Serna Gómez, J. H., Díaz-Piraquive, F. N., Muriel-Perea, Y. D. J. and Díaz Peláez, A., 2021. Advances, opportunities, and challenges in the digital transformation of HEIS in Latin America. *Radical Solutions for Digital Transformation in Latin American Universities: Artificial Intelligence and Technology 4.0 in Higher Education*, pp. 55–75.

Shah, I. A., 2022. Cybersecurity Issues and Challenges for E-Government During COVID-19: A Review. *Cybersecurity Measures for E-Government Frameworks*, pp. 187–222.

Tamer, H. and Knidiri, Z., 2023. University 4.0: Digital transformation of higher education evolution and stakes in Morocco. *American Journal of Smart Technology and Solutions*, *2*(1), pp. 20–28.

Ulven, J. B. and Wangen, G., 2021. A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), p. 39.