European Journal of Business and Management
ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online)
Vol.16, No.1, 2024

Addressing Cybersecurity and Privacy Concerns in E-Learning: Evidence from Kuwaiti Educational Sector

Abdullah Feraih Alenezi
College of Business Studies, Public Authority for Applied Education and Training,
7WG5+CW5, Ardiya, Kuwait
Email of corresponding author: Af.alenezi@paaet.edu.kw

Abstract
This study explored cybersecurity and privacy concerns within e-learning in the Kuwaiti educational sector. This is done through adopting a mixed-methods approach that incorporates an online questionnaire and semi-structured interviews. Quantitative data from 384 participants indicated moderate to high cybersecurity and privacy concerns. In order to explore further about such concerns, qualitative data were collected from 16 interviewees and highlighted key issues such as lack of awareness, platform security deficiencies, privacy worries and regulatory needs. To address these concerns, the study proposed a comprehensive "Kuwaiti Educational Cybersecurity and Privacy Assurance Framework" (KECPAF) centred around cybersecurity education, platform security enhancement, clear policy development and robust enforcement. The research calls for collective effort among stakeholders and collaboration with cybersecurity experts to effectively implement the framework, adapt to evolving threats and improve the security of e-learning platforms in Kuwait's educational sector.
Keywords: Kuwait, Education, e-learning, Cybersecurity, Privacy, Confidentiality, Framework.
DOI: 10.7176/EJBM/16-1-01
Publication date: January 31st 2024

1. Introduction

Rapid advancements in technology have triggered an accelerated shift from traditional face-to-face learning to online platforms (Renu, 2021). As such, e-learning has been considered extensively in the realm of education (Halili, 2019). This phenomenon has transcended borders with the Kuwaiti educational sector being no exception. Kuwait's experience, which represents a unique blend of the promise of e-learning; however, has been forged with potential pitfalls associated with it specially in the areas of cybersecurity (Alkharang and Ghinea, 2013).

Cybersecurity and privacy are issues of global concern and are particularly sensitive in the field of education (Anghel & Pereteanu, 2020). These concerns pertain to the safeguarding of personal data and information so as to shield against unauthorised access and maintaining confidentiality. Moreover, these issues extend beyond individuals to encompass institutional integrity and the preservation of a safe and conducive environment for learning (Rjaibi et al., 2012). As such, institutions are grappling with protecting sensitive data, educators are anxious about the confidentiality of their materials and students are often uncertain about the security of their personal information. The increasingly pervasive use of e-learning platforms also exposes the system to the risk of hacking, phishing, identity theft and other malicious activities that could jeopardize the education process (Kaur, 2020). Moreover, privacy issues are closely intertwined with these cybersecurity challenges. The concerns are about unauthorised access to data as well as the misuse of legitimate access (Alwi and Fan, 2010). For instance, intrusive tracking of student activities, profiling for commercial purposes, or the inappropriate use of data by authorised individuals could also compromise privacy (Khan et al., 2022). Despite the evident concerns, comprehensive studies examining these issues in the context of the Kuwaiti educational sector remain scarce (Eze et al., 2018). This gap in literature poses a significant problem. Without detailed research, stakeholders lack robust evidence to inform the design of policies, frameworks and interventions aimed at mitigating these risks. This study aims to shed light on these emerging challenges; mainly, a focus on the cybersecurity and privacy issues in Kuwait's e-learning context. It seeks to identify and understand the nature and extent of these problems, the factors contributing to them and their implications for students, educators, and institutions. It also aspires to propose practical solutions and recommendations for improving cybersecurity and privacy in e-learning within Kuwait which could serve as a blueprint for other regions facing similar challenges.

2. Literature review

2.1. Theoretical part: Frameworks in Cybersecurity and privacy

This paper will discuss three distinctive frameworks (i.e., Cybersecurity Control Frameworks; Cybersecurity Program Frameworks, and Cybersecurity Risk Frameworks) in an attempt to manifest the ways such frameworks deal with balance between cybersecurity and privacy issues.

Cybersecurity control frameworks provide a structured set of guidelines that define specific tasks that need to be performed to ensure the safety of the information systems. These controls are generally divided into various categories, such as administrative, physical, and technical controls. An example of a cybersecurity control

framework is the NIST (National Institute of Standards and Technology) Cybersecurity Framework. It consists of five core functions - identify, protect, detect, respond, and recover. It is a highly flexible and customizable framework that provides a risk-based approach to cybersecurity. These frameworks provide an organization with a clear structure and path to follow to ensure data and system protection. They cover a wide range of potential threats and offer a comprehensive, layered defence strategy. However, implementing these frameworks can be quite complex and time-consuming. Depending on the organization's size and complexity, it can also be expensive. They often require significant changes to current practices and require buy-in from all levels of the organisation.

Cybersecurity Program Frameworks focus on developing an overall program within an organization that addresses cybersecurity needs. These frameworks may include elements like creating a cybersecurity policy, developing a cybersecurity team, training and education, and incident response planning. The ISO 27001 is a well-known example of a Cybersecurity Program Framework. It provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system. These frameworks give a broader approach to cybersecurity and often include elements related to culture, employee behavior, and management commitment, all of which are critical to maintaining a robust cybersecurity posture. Nevertheless, just like the control frameworks, these can be complex and expensive to implement. It might be overkill for small businesses that don't face the same level of threats as a larger organisation. Moreover, ensuring continuous adherence to the framework can be challenging.

Cybersecurity risk frameworks are used to identify and evaluate the risk associated with cyber threats. They help in understanding and prioritizing risks, and this allows the organization to focus its resources on the most significant threats. The NIST SP 800-30 is an example of a risk management framework. It provides guidelines for conducting risk assessments, which includes steps such as identifying risks, assessing the risk, implementing risk responses, and monitoring risks. On the one hand, These frameworks help organisations focus on the most significant threats, which can make their cybersecurity efforts more efficient. They also provide a structured approach to risk management, which can be helpful for regulatory compliance. On the other hand, as with the other frameworks, these could be complex to implement. As such, they might require a significant investment of time and resources. Additionally, risk assessment is inherently subjective and different individuals may come to different conclusions about the level of risk associated with a particular threat.

It should be noted that these frameworks might be deemed useful for giving significant benefits; nevertheless, they are not without their challenges. Accordingly, the choice between them should be based on the specific needs and capabilities of the organisation. A holistic approach to cybersecurity often involves using elements from each of these frameworks to create a comprehensive security program that addresses the organisation's unique risks and vulnerabilities.

2.2. Practical Part: Past Studies

Addressing cybersecurity in e-learning is crucial for modern education. Bandara et al. (2014) performed a thorough analysis of cybersecurity concerns in e-learning through discussing threats like phishing, data breaches and malware. Due to e-learning platforms' open and information-sharing nature, they present unique security challenges. The researchers advocate for technical and educational strategies to mitigate risks and emphasise support cybersecurity culture among users. Ibrahim et al. (2020) explored cybersecurity challenges in e-learning and database management systems through examining the integrity and reliability of these platforms. Ibrahim et al. (2020) found that cyberattacks may disrupt but in severe cases it could halt operations of e-learning systems. The study illuminated specific security challenges such as SQL injection and cross-site scripting and propose future research on robust intrusion detection systems and recommending practices like regular updates and patches to enhance security. Rjaibi et al. (2012) examined cybersecurity measurements applicable to e-learning platforms through underscoring the necessity for SMART (Specific, Measurable, Actionable, Realistic, Time-bound) cybersecurity objectives. They suggested a model for measuring cybersecurity through including identifying key performance indicators, establishing a security baseline, and constantly monitoring and improving security practices. This work serves as a practical guide for enhancing and measuring cybersecurity in e-learning environments, providing valuable insights for future initiatives and strategies in the field.

The incessant evolution of digital learning platforms, heightened by the Covid-19 pandemic, has brought cybersecurity and privacy to the fore of e-learning discussions. The study of Buja (2021), Karagiannis et al. (2020) shed light on different facets of these pressing issues, encompassing policy level concerns, the role of educational tools, and a comprehensive security framework respectively.

Buja's (2021) article "Cyber Security Features for National E-Learning Policy" presents an illuminating viewpoint on how cybersecurity must be incorporated into national e-learning policy. Buja identifies an increasing need for policy-makers to understand and appreciate the role of cybersecurity in the successful implementation of e-learning initiatives. He suggests that a lack of clear-cut and robust cybersecurity features in a national e-learning policy could potentially jeopardise the e-learning program's overall success. Furthermore, the author emphasises the necessity of not just reactive but also proactive strategies that anticipate and guard against potential breaches.

Karagiannis et al (2020) take a more targeted, tool-oriented approach. They delve into the efficacy of Capture the Flag (CTF) platforms, a type of cybersecurity game used as a practical teaching method for computer security. The study's empirical analysis of various open-source CTF platforms reveals their significant potential in providing hands-on cybersecurity education. The authors highlight that while these tools can indeed be used to foster a deeper understanding of cybersecurity, they should not be seen as a panacea, as they might have limitations and could potentially be exploited if not properly managed.

Ali and Zafar's (2017) provides an overarching perspective on the issue, proposing a comprehensive security and privacy framework specifically tailored for e-learning environments. The proposed framework offers a balanced combination of technical measures (like encryption and intrusion detection systems), non-technical measures (like user training and policy enforcement), and governance considerations (like compliance and risk management). The authors argue that such a comprehensive framework is critical to protect both the integrity of the e-learning platform and the privacy of its users, thereby enabling a safe, efficient, and effective learning experience.

Aldhaferri (2016) critically examines Kuwait's E-learning environment through exploring technological, pedagogical, and organizational aspects related to public institutions' readiness for effective E-learning implementation. He notes a significant gap in cybersecurity strategies due to educators' limited technical knowledge and insufficient IT infrastructure which would make institutions susceptible to cyber threats and data privacy breaches. The study suggests that ensuring a secure E-learning implementation requires a deep understanding of cybersecurity measures, techniques, and potential threats. Furthermore, with E-learning platforms handling sensitive data, privacy protection is crucial. Aldhaferri advocates for clear privacy policies, robust encryption and stringent access controls in E-learning systems.

Alajmi et al. (2018) extend this discussion by exploring the adoption of cloud-based E-learning in higher education institutions in the GCC region. They find that these institutions adopted cloud-based E-learning without implementing adequate cybersecurity measures. This would expose them to substantial risks due to cloud services' vulnerability to cyber threats. The study reveals a lack of cybersecurity culture, insufficient security policies, standards and protocols for cloud-based E-learning which would increase cyber-attack risks. It further highlights privacy issues as many institutions fail to guarantee data privacy and confidentiality and such gaps related to privacy were attributed to weak encryption and inadequate security practices. Both studies (i.e., Alajmi et al., 2018; Aldhaferri, 2016) underscore the need for enhanced cybersecurity and privacy measures in E-learning environments as well as recommending future work focus on cultivating strong cybersecurity cultures, strategies and technologies along with rigorous privacy controls to establish a secure E-learning framework.

The reviewed literature indicates a growing concern about cybersecurity in e-learning, stressing the need for technical, educational, and strategic solutions. Bandara et al. (2014) emphasise the importance of user education and awareness, Ibrahim et al. (2020) highlight the need for technical measures such as intrusion detection systems and regular updates, while Rjaibi et al. (2012) underline the need for concrete and measurable cybersecurity objectives. Collectively, these studies emphasise that addressing cybersecurity in e-learning requires a holistic approach that combines awareness, technical measures, and strategic planning. The existing literature highlights the multifaceted nature of cybersecurity and privacy concerns in e-learning. It underscores the need for a synergistic approach that combines policy-level considerations and innovates educational tools as well as considers comprehensive frameworks to effectively address these concerns. The convergence of these facets would be key to harnessing the full potential of e-learning while ensuring the security and privacy of all stakeholders. This area remains ripe for further research, particularly with regard to the development and empirical testing of more sophisticated security mechanisms, tools, and policy recommendations.

3. Methodology

3.1. Study Design

This research adopts a mixed-methods approach that uses both quantitative and qualitative methods. This approach allows for a more comprehensive examination of the cybersecurity and privacy concerns within the e-learning environment in the Kuwaiti educational sector (Almpanis, 2016).

3.2. Population and Sample

The target population of this study comprises educators, students, IT staff, and administrators within the Kuwaiti educational sector who have interacted with e-learning platforms. Given the vast number of potential participants, a stratified random sampling technique is employed. The population is divided into four groups: educators, students, IT staff, and administrators (Ayeni, 2012). A random sample is taken from each group so as to ensure representation across different schools and institutions, roles, and experience levels with e-learning platforms (Ayeni, 2012).

3.3. Data Collection

In regard to quantitative data collection, an online questionnaire is created which includes sections on unidentifiable personal details of gender, age, and qualification. Other sections contain questions related to familiarity with e-learning, and specific questions on cybersecurity and privacy concerns. The questionnaire is divided into two parts. The first part deals with demographics and general experience with e-learning, while the second part consists of a Likert-scale assessment so as to allow respondents to rate their experience and perceptions of cybersecurity and privacy within e-learning environments. The questionnaire is distributed through institutional emails and social media groups related to the Kuwaiti educational sector. In addition, an explanatory letter is attached so as to state the purpose of the study, the voluntary nature of participation and the assurances of anonymity and confidentiality.

Regarding qualitative data collection, following the analysis of the survey results, semi-structured interviews are conducted with a select group of participants (comprising of educators, students, IT staff, and administrators). The interviews are used to delve deeper into specific concerns and experiences raised in the survey responses so as to identify potential solutions and suggestions for improving cybersecurity and privacy in e-learning. The interview questions are prepared in advance but were flexible enough to allow further probing based on the responses of participants.

3.4. Inclusion and Exclusion Criteria

To be eligible for this study, participants should have had direct interaction with e-learning platforms within the Kuwaiti educational sector. This includes educators who have conducted classes online, students who have participated in online learning, IT staff who manage and support these platforms, and administrators who oversee the implementation and use of e-learning. Participants who have not interacted with e-learning platforms in the Kuwaiti educational sector, those unwilling to participate voluntarily and individuals below the age of 18 are excluded from this study.

3.5. Recruitment of Participants

Potential participants are approached through their institutional emails, wherein they are informed about the study and invited to participate. Participation in the study is voluntary with no incentives offered. It is made clear to potential participants that they could withdraw from the study at any time without any consequences.

3.6. Data Analysis

The collected data from the questionnaires is analysed using descriptive and inferential statistical analysis such as means, standard deviations, and correlations. The qualitative data from the interviews is transcribed and analysed thematically. The themes identified were used to gain a deeper understanding of the cybersecurity and privacy concerns in e-learning in the Kuwaiti educational sector. Quantitative and qualitative data were then integrated to form a comprehensive picture of the issue at hand.

4. Findings

In this research, the total number of participants is 427. The response rate for the distributed online questionnaire was high (89.92% as the sample size was 384) which show that there is substantial interest and engagement with the subject of cybersecurity and privacy concerns within e-learning in the Kuwaiti educational sector (Fan and Yan, 2010).

Cronbach's alpha is a measure of internal consistency or reliability, and it is generally used in social science research. It varies between 0 and 1, with higher values indicating better internal consistency.

Scale	No. of Items	Sample Size	Cronbach's Alpha
Cybersecurity Concerns	10	384	0.82
Privacy Concerns	10	384	0.80

Table 1: Cronbach's Alpha

In the Likert-scale questionnaire which is distributed to participants, both scales of Cybersecurity Concerns and Privacy Concerns consist of 10 items each. The Cronbach's Alpha values for both scales are acceptable as they are above 0.7 (table 1). This indicates that the items have relatively high internal consistency.

Analysis of the demographic data revealed a balanced representation across different roles in the educational sector (table 2).

Role	Percentage	Cybersecurity Concerns (Mean ± SD)	Privacy Concerns (Mean ± SD)
Educators	24%	3.8 ± 1.3	4.2 ± 1.1
Students	30%	4.0 ± 1.2	4.0 ± 1.2
IT Staff	22%	3.7 ± 1.1	4.3 ± 1.0
Administrators	24%	3.9 ± 1.2	4.1 ± 1.1
Overall	100%	3.9 ± 1.2	4.1 ± 1.1

Table 2: Demographic Data and Concern Ratings

The sample was composed of educators (24%), students (30%), IT staff (22%), and administrators (24%). In the Likert-scale assessment, respondents were asked to rate their perceived level of cybersecurity and privacy within e-learning environments. The majority of respondents expressed moderate to high concerns about cybersecurity (mean score = 3.9, standard deviation = 1.2) and privacy (mean score = 4.1, standard deviation = 1.1). This suggests a noticeable level of concern and apprehension among stakeholders about the safety of e-learning platforms. Table 2 shows that IT Staff has the lowest cybersecurity concerns and the highest privacy concerns, while students have equal concern levels for both cybersecurity and privacy.

In the cybersecurity concerns items, participants generally demonstrated significant apprehension (table 3).

Item	**Mean**	**SD**
Secure login procedures	4.1	0.9
Protection from malware	4.0	1.0
Data encryption	4.2	1.0
Secure network connection	3.9	1.1
Regular security updates	4.0	1.0
Use of strong passwords	4.2	0.9
Two-factor authentication	4.1	1.0
Protection from phishing attacks	3.9	1.1
Confidentiality of personal data	4.1	1.0
Knowledge of security protocols	4.0	0.9

Table 3: Cybersecurity Concerns

According to table 3, high scores (mean >4) across a broad range of security aspects like secure login procedures, data encryption, and two-factor authentication reflect a pervasive sense of unease. Regular security updates and protection from phishing attacks received the lowest, albeit still considerable, scores (mean ~4). This suggests areas for potential improvement in e-learning platforms. Notably, respondents showed high confidence (mean 4.2) in the use of strong passwords which signifies an area where effective practices are being adopted. These findings underline the critical need for bolstering cybersecurity measures in e-learning environments.

The results in Table 4 convey significant privacy concerns amongst the participants. All aspects of privacy, including control over personal data, confidentiality of communication, and rights to data deletion scored highly (mean >4).

Item	**Mean**	**SD**
Data privacy policies	4.2	0.9
Control over personal data	4.1	0.9
Anonymity assurance	4.3	1.0
Confidentiality of communication	4.1	1.1
Consent for data collection	4.2	0.9
Transparency of data usage	4.3	1.0
Non-disclosure of personal information	4.1	0.9
Protection from unauthorised data access	4.0	1.0
Data breach notifications	4.2	1.0
Rights to data deletion	4.3	0.9

Table 4: Privacy Concerns

Based on table 4, it is mainly noteworthy that the aspect of 'anonymity assurance' and 'transparency of data usage' elicited the greatest concern (mean 4.3). This does reflect the participants' desire for more transparent data handling. The 'protection from unauthorised data access' received a slightly lower score (mean 4.0); yet remains significant. This points towards necessary improvements in this area. These findings emphasise the pressing need for e-learning platforms to enhance privacy measures and to communicate these effectively to users.

Qualitative Findings were collected from 16 interviewees. The semi-structured interviews and textual data were analysed through using thematic analysis of (Braun and Clarke, 2014). The results provided more detailed insight into the specific concerns and experiences of stakeholders. Major themes that emerged were (i.e., lack of awareness and training, platform security, privacy concerns, policy and regulation). Lack of Awareness and

Training: Many participants, mainly educators and students, expressed a lack of understanding of cybersecurity threats and privacy risks in the e-learning environment. They expressed the need for more education and training in this regard. The 1st teacher said that *"I do not know exactly how to deal with privacy issues in online teaching and how such privacy can be undermined"*. Platform Security: IT staff and administrators noted that some e-learning platforms employed by the institutions had inadequate security measures. They noted instances of data breaches and unauthorised access. According to one of the IT participants, *"some users of e-learning do keep their website open after usage without logging off which would enable anybody to see confidential details"*. Privacy Concerns: Students and educators raised concerns over the privacy of their communications and the handling of their personal information in e-learning platforms. According to a student at university, *"I am a women and I am very sensitive that my personal detains will be kept confidential ; but, I am afraid from third party persons who might get access to my details in online education"*. Policy and Regulation: Participants across all groups highlighted the need for clear policies and regulations related to cybersecurity and privacy in e-learning. It was also noted that there was a lack of consistent enforcement of these policies. According to another teacher, *"decision makers in educational sector in Kuwait should clearly embrace laws that assure privacy and security in online teaching and e-learning"*

The integration of quantitative and qualitative findings has provided a comprehensive overview of the situation. On the one hand, the quantitative data showed the overall level of concern regarding cybersecurity and privacy within e-learning environments. On the other hand, the qualitative data elucidated the specific nature of these concerns. There is a significant demand for enhanced cybersecurity measures and privacy protections within the e-learning context in the Kuwaiti educational sector. The findings underscore the need for increased awareness and training on cybersecurity and privacy, buttressed security measures in e-learning platforms and the development and enforcement of clear policies and regulations. These findings provide a robust evidence base for guiding interventions to enhance cybersecurity and privacy in the e-learning environment in the Kuwaiti educational sector. They point to the need for a multi-faceted approach that involves improving system security, affording education and training for all stakeholders and developing and enforcing clear and effective policies and regulations.

5. Discussion

The findings of the study underscore a pervasive concern among stakeholders in Kuwait's educational sector regarding cybersecurity and privacy within e-learning environments. There is a noticeable apprehension with participants expressing moderate to high concerns. This is an indicative of an immediate call for action to alleviate these fears. Quantitative data reveal the general climate of concern and highlight areas demanding particular attention. The qualitative data complement these findings by providing a deeper understanding of specific issues stakeholders encounter so as to frame a more comprehensive picture of the existing concerns. A significant theme emerging from the study is the lack of awareness and training among educators and students regarding cybersecurity threats and privacy risks. The participants' narratives illustrate a tangible knowledge gap that underscore the imperative for educational initiatives to improve understanding and competency in navigating e-learning platforms securely. Addressing this knowledge gap is crucial as it forms the foundation for creating a secure e-learning environment where users are not only passive beneficiaries of security protocols but active participants in maintaining a secure digital learning space. Moreover, concerns related to platform security were evident. This is pointing towards a need for robust security measures on e-learning platforms currently in use. Stakeholders reported instances of data breaches and unauthorized access which are serious issues that could undermine the trust and reliability of e-learning in the educational sector. It is essential for educational institutions to invest in secure e-learning infrastructures, routinely conduct security assessments and implement necessary updates and enhancements to address security deficiencies. Participants further articulated concerns regarding privacy mainly the confidentiality of communications and handling of personal information. These concerns are valid considering the sensitive nature of the data handled by e-learning platforms. It is imperative for providers to ensure the highest level of data protection to preserve the integrity of the learning process and protect users from potential harms associated with data breaches or unauthorized access. Furthermore, the study revealed that there is a need for clear, coherent policies and stringent regulations that uphold cybersecurity and privacy standards. The participants' thought call attention to the absence of such policies and the inconsistent enforcement where policies do exist. This policy vacuum and enforcement gap underscore an urgent need for a regulatory framework that offers clear guidelines and is backed by effective enforcement mechanisms to safeguard the interests of all stakeholders in the e-learning environment. The findings of the current research align with and extend the work of previous studies, offering a granular look at the challenges posed by cybersecurity and privacy concerns in e-learning within the Kuwaiti educational sector. A salient theme that emerged from this research is the significant demand for enhanced cybersecurity measures and privacy protections, which is congruent with the global discourse on e-learning (Bandara et al., 2014; Anghel & Pereteanu, 2020). Our quantitative data, demonstrating a pervasive concern about cybersecurity and privacy across different stakeholders in education, echoes the results

of prior studies. Similar to the work of Ibrahim et al. (2020), this study also emphasises the need for improved security features in e-learning platforms to mitigate these concerns. From the qualitative findings, the theme of lack of awareness and training resonates with previous literature. Aldhaferri (2016) underscores the significance of meaningful e-learning implementation and readiness, which inherently requires a solid understanding of potential threats and how to mitigate them. It is evident that to foster confidence in e-learning systems, there is a pressing need for substantial education and training about cybersecurity threats and privacy risks. The results further highlight issues concerning the security of e-learning platforms. This aligns with Ali and Zafar's (2017) argument for a comprehensive security and privacy framework for e-learning. The experience of unauthorised access and data breaches reported by participants echoes the potential threats identified by Rjaibi et al. (2012), reinforcing the necessity for robust security measures. Furthermore, the privacy concerns expressed by students and educators in this study echo the work of Buja (2021), who emphasised the importance of integrating cybersecurity features into national e-learning policies. The apprehensions about the privacy of communication and handling of personal data in e-learning platforms call for immediate attention and action. Moreover, the identified need for clear policies and regulations, alongside consistent enforcement, finds support in the study of Karagiannis et al. (2020). Their analysis advocates for comprehensive cybersecurity e-learning tools, emphasising that an understanding of policy and regulation is fundamental to addressing cybersecurity challenges effectively.

The use of the Cybersecurity Control, Program, and Risk Frameworks to guide the study's analysis brought to the fore a range of issues regarding e-learning security in Kuwait. Notably, despite these frameworks' broad application in previous studies (Anghel & Pereteanu, 2020; Alajmi et al., 2018), the current findings indicate a gap in their implementation within the Kuwaiti educational sector. This research's findings point to the necessity of a multi-faceted approach to cybersecurity in e-learning. It underscores the need for stronger system security, comprehensive education and training for all stakeholders and the development and consistent enforcement of clear and effective policies and regulations. This research provides substantial groundwork for the continued exploration of these areas and for the development of targeted interventions within the Kuwaiti educational sector.

5.1. Research implications

Based on the findings and discussion of this study, this paper proposes a new comprehensive framework called the "Kuwaiti Educational Cybersecurity and Privacy Assurance Framework" (KECPAF) to address cybersecurity and privacy concerns in e-learning in the Kuwaiti educational sector. This framework has four main pillars:

I. Cybersecurity Education and Training: Given the lack of awareness and understanding of cybersecurity threats and privacy risks, a strong focus should be placed on education and training which has been already mentioned in studies of (Catota et al., 2019 and Venter et al., 2019) . This should involve creating awareness programs and curricula for all stakeholders - students, educators, IT staff, and administrators (Catota et al., 2019). Training should cover issues related to identifying common threats, implementing basic protective measures and understanding the importance of cybersecurity practices in the e-learning environment (Rahman et al., 2020).

II. Enhanced E-learning Platform Security: A considerable part of the framework will focus on improving the security of e-learning platforms as suggested by (Bandara et al., 2014). This involves conducting regular security audits of these platforms and ensuring they meet the most up-to-date cybersecurity standards (Masud and Huang, 2012). This process should also focus on implementing strict access controls to prevent unauthorised access, securing databases to avoid data breaches and employing robust encryption techniques to ensure data privacy (Durairaj and Manimaran, 2015).

III. Clear Policies and Regulations: Developing clear and concise policies and regulations that guide all cybersecurity and privacy practices is essential as suggested by (Buja, 2021). These should encompass acceptable use policies, data privacy policies, and incident response plans (Buja, 2021). In addition, according to Anghel and Pereteanu (2020) policies should be straightforward and readily accessible so as to make them easy for all stakeholders to understand and comply with.

IV. Enforcement and Monitoring: The framework also needs to include stringent enforcement mechanisms to ensure adherence to policies and regulations (Barik and Karforma, 2012). Regular audits should be conducted to check compliance and punitive measures should be in place for non-compliance. In addition, there should be continuous monitoring of the e-learning environment to detect and respond to potential cybersecurity threats promptly (Favale et al., 2020).

KECPAF's success relies substantially on the collective effort of all stakeholders. The IT staff and administrators have to ensure the implementation of secure systems and enforcement of policies. At the same time, educators and students have a role to play by adhering to these policies and participating actively in the cybersecurity education and training programs. Furthermore, for the successful implementation of this framework, it is suggested that the Kuwaiti educational sector should collaborate with cybersecurity experts and relevant government bodies. This collaboration will ensure that the framework aligns with national cybersecurity strategies and maintains relevance with evolving cybersecurity threats. Moreover, it should be assured that KECPAF should

be dynamic, adapting to the fast-paced changes in the cybersecurity landscape. Regular review and updates of the framework are crucial to ensuring it remains effective and applicable in protecting the e-learning environment in the Kuwaiti educational sector against current and future cybersecurity and privacy concerns.

6. Conclusion

The current study provides a broad understanding of the cybersecurity and privacy concerns within the Kuwaiti educational sector's e-learning environment through using a mixed-methods approach. The quantitative and qualitative analyses have revealed a range of issues, including the lack of comprehensive cybersecurity measures, insufficient awareness among users and potential privacy breaches.

6.1. Limitations

Despite the insightful findings, the study is not without its limitations. First, the data collected relies heavily on self-reported measures which may be influenced by social desirability bias (Larson, 2019). Respondents may have answered in ways they believe are socially acceptable rather than reflecting their true experiences or perceptions (Larson, 2019). Second, while the stratified random sampling technique was used to ensure representation across different groups, the sample may not be truly representative of the Kuwaiti educational sector as a whole due to the voluntary nature of participation (Sharma, 2017). Those with a particular interest in or concern about cybersecurity and privacy may have been more likely to participate which may have skewed the results (Westreich, 2012). Thirdly, the study was restricted to individuals who have interacted with e-learning platforms within the Kuwaiti educational sector. Therefore, the findings may not be generalisable to other regions, sectors, or individuals who have not used such platforms (Murad et al., 2018).

6.2. Future Recommendations

Despite these limitations, the study offers valuable insights that could guide future research and practice. For future research, it is recommended to incorporate other data collection methods such as observations or audits of the e-learning systems to provide a more objective assessment of cybersecurity measures (Farrington, 2014). Moreover, future studies could explore the use of experimental or longitudinal designs to assess causal relationships and changes over time (Klement, and Dostál, 2014). In terms of practice, institutions in the Kuwaiti educational sector should consider enhancing their cybersecurity infrastructure and incorporating more rigorous privacy protections. Moreover, it is essential to raise awareness among users about potential cybersecurity threats and privacy issues, along with strategies to protect themselves. Furthermore, the inclusion of cybersecurity and privacy courses or modules within the curriculum may be beneficial. This could equip students and staff with the necessary skills to navigate e-learning platforms safely and effectively. To conclude, cybersecurity and privacy concerns in e-learning represent a crucial issue that requires ongoing attention and action from educators, administrators, IT staff and students alike. This research marks a significant step towards understanding and addressing these concerns in the Kuwaiti educational sector through setting a foundation for continued research and improvement.

References

Alajmi, Q., Arshah, R.A., Kamaludin, A. and Al-Sharafi, M.A., 2018, November. Current state of cloud-based e-learning adoption: Results from Gulf Cooperation Council's Higher Education Institutions. In *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 569-575). IEEE.

Aldhaferri, F.M., 2016. E-Learning Readiness in Public Institutions. In *Revolutionizing Modern Education through Meaningful E-Learning Implementation* (pp. 245-265). IGI Global. DOI: 10.4018/978-1-5225-0466-5.ch013

Ali, R. and Zafar, H., 2017. A security and privacy framework for e-Learning. *International Journal for e-Learning Security*, 2046-4568.

Alkharang, M.M. and Ghinea, G., 2013. E-learning in higher educational institutions in Kuwait: Experiences and challenges. *International Journal of Advanced Computer Science and Applications*, *4*(4).

Almpanis, T., 2016. Using a mixed methods research design in a study investigating the 'Heads of e-Learning'perspective towards Technology Enhanced Learning. *Electronic Journal of e-Learning*, *14*(5), pp.pp301-311.

Alwi, N.H.M. and Fan, I.S., 2010. E-learning and information security management. *International Journal of Digital Society (IJDS)*, *1*(2), pp.148-156.

Anghel, M. and Pereteanu, G.C., 2020. Cyber Security Approaches in E-Learning. In *INTED2020 Proceedings* (pp. 4820-4825). IATED.

Ayeni, A.J., 2012. Assessment of Principals' Supervisory Roles for Quality Assurance in Secondary Schools in Ondo State, Nigeria. *World Journal of Education*, *2*(1), pp.62-69.

Bandara, I., Ioras, F. and Maher, K., 2014. Cyber security concerns in e-learning education.

Barik, N. and Karforma, S., 2012. Risks and remedies in e-learning system. *arXiv preprint arXiv:1205.2711*.

Braun, V. and Clarke, V., 2014. What can "thematic analysis" offer health and wellbeing researchers?. *International journal of qualitative studies on health and well-being*, *9*(1), p.26152. https://doi.org/10.3402/qhw.v9.26152

Buja, A.G., 2021. Cyber Security Featuresfor National E-Learning Policy. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(5), pp.1729-1735.

Catota, F.E., Morgan, M.G. and Sicker, D.C., 2019. Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), p.tyz001.

Durairaj, M. and Manimaran, A., 2015. A study on security issues in cloud based e-learning. *Indian Journal of Science and Technology*, *8*(8), pp.757-765. DOI: 10.17485/ijst/2015/v8i8/69307

Eze, S.C., Chinedu-Eze, V.C. and Bello, A.O., 2018. The utilisation of e-learning facilities in the educational delivery system of Nigeria: a study of M-University. *International Journal of Educational Technology in Higher Education*, *15*(1), pp.1-20. https://doi.org/10.1186/s41239-018-0116-z

Fan, W. and Yan, Z., 2010. Factors affecting response rates of the web survey: A systematic review. *Computers in human behavior*, *26*(2), pp.132-139. https://doi.org/10.1016/j.chb.2009.10.015

Farrington, C.J., 2014. Blended e-learning and end of life care in nursing homes: a small-scale mixed-methods case study. *BMC palliative care*, *13*, pp.1-16. https://doi.org/10.1186/1472-684X-13-31

Favale, T., Soro, F., Trevisan, M., Drago, I. and Mellia, M., 2020. Campus traffic and e-Learning during COVID-19 pandemic. *Computer networks*, *176*, p.107290. https://doi.org/10.1016/j.comnet.2020.107290

Halili, S.H., 2019. Technological advancements in education 4.0. *The Online Journal of Distance Education and e-Learning*, *7*(1), pp.63-69.

Ibrahim, H., Karabatak, S. and Abdullahi, A.A., 2020, June. A study on cybersecurity challenges in e-learning and database management system. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

Karagiannis, S., Maragkos-Belmpas, E. and Magkos, E., 2020. An analysis and evaluation of open source capture the flag platforms as cybersecurity e-learning tools. In *Information Security Education. Information Security in Action: 13th IFIP WG 11.8 World Conference, WISE 13, Maribor, Slovenia, September 21–23, 2020, Proceedings 13* (pp. 61-77). Springer International Publishing.

Kaur, M.S., 2020. A Review Paper on Ethical Hacking-E-Learning Case Study. *New Paradigm in eLearning Technologies Arising Due To Covid-19 Crisis*, p.25. DOI: 10.34218/IJARET.11.12.2020.018

Khan, A.R., Khosravi, S., Hussain, S., Ghannam, R., Zoha, A. and Imran, M.A., 2022, March. Execute: Exploring eye tracking to support e-learning. In *2022 IEEE Global Engineering Education Conference (EDUCON)* (pp. 670-676). IEEE. **DOI:** 10.1109/EDUCON52537.2022.9766506

Klement, M. and Dostál, J., 2014. Students and e-learning: A Longitudinal Research Study into University Students' Opinions on e-learning. *Procedia-Social and Behavioral Sciences*, *128*, pp.175-180. https://doi.org/10.1016/j.sbspro.2014.03.139

Larson, R.B., 2019. Controlling social desirability bias. *International Journal of Market Research*, *61*(5), pp.534-547. https://doi.org/10.1177/1470785318805305

Masud, M. and Huang, X., 2012. An e-learning system architecture based on cloud computing. *World Academy of Science, Engineering and Technology*, *62*, pp.74-78.

Murad, M.H., Katabi, A., Benkhadra, R. and Montori, V.M., 2018. External validity, generalisability, applicability and directness: a brief primer. *BMJ evidence-based medicine*, *23*(1), p.17. DOI:10.1136/ebmed-2017-110800

Rahman, N.A.A., Sairi, I., Zizi, N.A.M. and Khalid, F., 2020. The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), pp.378-382. doi: 10.18178/ijiet.2020.10.5.1393

Renu, N., 2021. Technological advancement in the era of COVID-19. *SAGE Open Medicine*, *9*, p.20503121211000912. Ds:O//dIo: i10.177/2050312110912

Rjaibi, N., Rabai, L.B.A., Aissa, A.B. and Louadi, M., 2012. Cyber security measurement in depth for e-learning systems. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, *2*(11), pp.107-120.

Sharma, G., 2017. Pros and cons of different sampling techniques. *International journal of applied research*, *3*(7), pp.749-752.

Venter, I.M., Blignaut, R.J., Renaud, K. and Venter, M.A., 2019. Cyber security education is as essential as "the three R's". *Heliyon*, *5*(12), p.e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

Westreich, D., 2012. Berkson's bias, selection bias, and missing data. *Epidemiology (Cambridge, Mass.)*, *23*(1), p.159. doi: 10.1097/EDE.0b013e31823b6296