frontiers | Frontiers in Communication

TYPE Original Research
PUBLISHED 08 July 2025
DOI 10.3389/fcomm.2025.1552520

OPEN ACCESS

EDITED BY
Nicola Mucci,
University of Florence, Italy

REVIEWED BY
Gaurav Kumar,
GLA University, India
Marius Laurinaitis,
Mykolas Romeris University, Lithuania
Shuruq Alsharif,
Imam Abdulrahman Bin Faisal University, Saudi Arabia

*CORRESPONDENCE
Mohammad Qudah
✉ mqudah5555@gmail.com;
✉ odeh.mohamad55@gmail.com

RECEIVED 28 December 2024
ACCEPTED 27 May 2025
PUBLISHED 08 July 2025

CITATION
Murad HA and Qudah M (2025) The attitudes of communicators toward cybersecurity concerning security, safety in national institutions.
Front. Commun. 10:1552520.
doi: 10.3389/fcomm.2025.1552520

The attitudes of communicators toward cybersecurity concerning security, safety in national institutions

Husain A. Murad[1] and Mohammad Qudah[2]*

[1]Mass Communication Department, College of Arts, Kuwait University, Kuwait City, Kuwait, [2]Faculty of Mass Communication, Radio and TV Department, Yarmouk University, Irbid, Jordan

This study aimed to assess the attitudes of communicators towards cybersecurity in relation to national security and safety standards in Kuwait. The study examined key factors influencing communicators' use of cybersecurity technologies. It also analyzed the legislation regulating this field. Additionally, it explored how these laws are used to shape media and public messages that promote national security and safety. To achieve this, the study followed a quantitative descriptive approach, using a questionnaire as the primary tool. The questionnaire was distributed to a sample of 140 communicators in Kuwaiti national institutions. The study found that Kuwaiti national institutions have laws and legislation related to cybersecurity. These regulations are linked to cybersecurity management and are continuously updated to meet digital and media transformation needs. The results also highlighted the presence of laws designed to curb spam messages. Also, a computer emergency response team is in place. However, communicators use different approaches to tackle cybersecurity threats, leading to a noticeable disparity in their methods. The study identified several key methods for raising cybersecurity awareness. One approach was using social media to educate the public. Another involved organizing lectures and seminars on cybersecurity. Additionally, meetings with specialists were held to increase awareness among school students. Furthermore, to strengthen cybersecurity readiness in national institutions, the study offers several actionable recommendations. These include integrating communicators into cybersecurity decision-making processes, enhancing training programs tailored to their roles, and fostering stronger collaboration between technical experts and communicators to ensure effective information dissemination. Moreover, national institutions should prioritize cybersecurity awareness campaigns, incorporate communicators in incident response planning, and adopt structured policies that align legislative frameworks with practical enforcement strategies. These measures will not only improve institutional cybersecurity resilience but also empower communicators to play a proactive role in mitigating cyber threats. In addition, this study recommends participating in knowledge exchange platforms, attending conferences, and enhancing awareness of media messages to benefit from collective experience and share best practices. It also suggests giving communicators priority in media measures, such as responding to threats or engaging with stakeholders. Hence, communication and media strategies in the field of cybersecurity should be integrated and activated more effectively across different media platforms.

KEYWORDS

organizational communication, cybersecurity, safety, national institutions, social systems, awareness, Kuwait, CERT

Introduction

Cybersecurity is a major concern in the twenty-first century. It protects systems and networks from digital attacks by cybercriminals (Al-Amiri, 2024). These attacks not only target technology but also pose risks to communicators, particularly in security, economic, and political institutions (Mijwil et al., 2023). Cybersecurity issues are now a global concern at the highest levels, posing significant security threats that lead to the penetration of data and information across various fields, thereby impacting national security, economic stability, and public trust (Khader et al., 2021; Pawar and Palivela, 2022). Moreover, the growing dependence on digital networks has significantly increased the risk of cyberattacks on national institutions (Ben Jeddou, 2022). In 2023, cyberattacks on government and public institutions worldwide rose by more than 38%. About 61% of these incidents were linked to phishing and social engineering attacks (Dawson et al., 2023). In Kuwait, cybersecurity incidents have risen by 42% over the past 3 years, primarily targeting sensitive sectors such as finance, healthcare, and public services (Tahat and Al-Mutairi, 2022). This alarming trend has received little attention regarding the role of communicators. These professionals serve as a vital link between technical experts and the general public. Communicators play a pivotal role in shaping institutional responses and public awareness, making their attitudes toward cybersecurity a crucial factor in the success of security strategies (Albannai et al., 2024). Effective communication is necessary to ensure that cybersecurity measures are understood and implemented properly (Trigeassou, et al., 2011; Al-Hamad, 2023). However, there is a research gap in understanding the specific roles, attitudes, and preparedness of communicators in managing cyber threats (Sen 1994; Trigeassou, et al., 2011).

To fully understand the relevance of cybersecurity in national institutions, it is essential to examine the broader context of cybersecurity frameworks, national policies, and their role in institutional security. National institutions play a crucial role in protecting a country's sovereignty and digital infrastructure, ensuring the continuity of public services, maintaining the integrity of sensitive data, and protecting vital operations (Eyadat, 2024). In recent years, rapid technological and communication advancements have increased reliance on digital networks and electronic systems (Shawirb and Murad, 2023). As a result, cybersecurity has become a major challenge for national institutions worldwide (Gao et al., 2023). As institutions modernize, they increasingly adopt emerging technologies such as cloud computing, big data, artificial intelligence, and the Internet of Things (IoT). Consequently, concerns over cybersecurity have also intensified. In Kuwait, cybersecurity has become a national priority. Institutions handle highly sensitive information in key sectors such as national security, healthcare, finance, and public services (Han and Zhang, 2020). Cyberattacks on these institutions disrupt vital operations. Moreover, they jeopardize national gains and undermine public trust (Enaya and Enaya, 2014). Recognizing these challenges, Kuwait has taken significant steps to enhance its cybersecurity framework (Sen, 1994; Al-Janafawi, 2023). One major initiative is the establishment of specialized bodies like the Communications and Information Technology Regulatory Authority (CITRA). These bodies develop policies and legislation to safeguard the country's cyberspace and address increasing vulnerabilities linked to digital transformation (Mijwil et al., 2023).

Despite these advancements, national institutions in Kuwait still face cybersecurity risks. The primary causes are gaps in institutional readiness and awareness. Previous studies highlight a lack of focus on the role of cybersecurity communicators. These professionals serve as a crucial link between technical experts, institutional leadership, and the general public (Murad, 2023). Organizational communicators hold significant responsibility in managing information, directing public opinion, and raising cybersecurity awareness within and beyond their institutions. However, research indicates that communicators' roles often remain limited to traditional communication tasks, without adequately addressing the technical dimensions of cybersecurity. This gap can lead to vulnerabilities that attackers may exploit (Khader et al., 2021; Tahat and Al-Mutairi, 2022).

Traditionally, cybersecurity has been viewed as a technical field. However, it is now recognized as a multidisciplinary domain. Effective cybersecurity requires both technical defenses and strategic communication. Organizations and the public must understand and respond appropriately to cyber threats (Dawson, 2018). As cyber threats become more complex, effective communication is increasingly important. Cybersecurity professionals must convey technical information to non-technical stakeholders (Han and Zhang, 2020). In this respect, communicators play a crucial role in cybersecurity. They help prevent data manipulation, misinformation, and information theft. Additionally, they mitigate risks to national, economic, societal, and intellectual security (Sharma and Maurya, 2020).

In Kuwait, the establishment of the Cybersecurity and Emergency Response Center in 2022 demonstrates the growing recognition of cybersecurity's importance (Štitilis et al., 2020). However, despite these advancements, gaps remain in communicators' understanding of cybersecurity and their integration into institutional strategies. This underscores the need to assess their preparedness and attitudes to develop effective cybersecurity strategies tailored to national institutions.

Despite the increasing importance of cybersecurity in Kuwaiti national institutions, there is a lack of research on the role and preparedness of communicators in addressing cyber threats. Most cybersecurity strategies focus on technological solutions, overlooking the significance of human factors in cybersecurity awareness, compliance, and crisis management. The absence of structured training programs and legislative support for communicators further exacerbates this issue. This study addresses these gaps by analyzing the attitudes, knowledge, and preparedness of communicators in Kuwaiti national institutions regarding cybersecurity.

The purpose of this study is to evaluate the attitudes of communicators in Kuwaiti national institutions toward cybersecurity and identify the factors influencing their effectiveness in promoting security measures and mitigating cyber threats. This research aims to assess their awareness of relevant legislation, preparedness for emerging threats, and role in shaping institutional and public responses. By bridging the gap between policy, practice, and communication, the study seeks to provide actionable recommendations for enhancing cybersecurity preparedness at the national level.

This study directly addresses the research topic by exploring how communicators in Kuwaiti national institutions perceive cybersecurity, their role in implementing security protocols, and the challenges they face in promoting cybersecurity awareness. Given that communicators serve as intermediaries between technical experts and the public, their attitudes and preparedness significantly influence national

cybersecurity resilience. This study also assesses the extent to which cybersecurity laws and institutional policies support communicators in fulfilling their roles. By integrating the Technology Acceptance Model (TAM), the research evaluates key factors influencing communicators' willingness to adopt cybersecurity practices, providing a comprehensive understanding of their contributions to national security strategies.

This study fills the research gap by examining how communicators in Kuwaiti national institutions perceive and respond to cybersecurity challenges. It provides actionable insights to improve institutional preparedness. Additionally, this study holds theoretical and practical importance. It integrates the Technology Acceptance Model (TAM) to examine communicators' attitudes, bridging a gap in existing literature that prioritizes technical solutions while neglecting the critical role of communication (Dawson et al., 2023). Also, the findings provide actionable recommendations for policymakers, organizational leaders, and cybersecurity trainers, emphasizing the importance of empowering communicators to shape effective cybersecurity strategies aligned with global standards (Tahat and Al-Mutairi, 2022). Finally, this research offers originality by being one of the first to explicitly examine the attitudes of communicators toward cybersecurity in Kuwaiti national institutions. Thus, building on this foundation, a review of existing literature in the next section provides critical insights into global cybersecurity challenges, legislative efforts, and the role of communicators in mitigating cyber threats.

Literature review

The following section evaluates previous research findings, highlighting key theoretical perspectives and identifying gaps that this study seeks to address.

To begin with, recognizing potential cybersecurity risks is essential for communicators and end-users. It informs strategic responses to threats. Howard and Cambria et al. (2022) emphasized that identifying risks in cyberspace is crucial for the safe use of information and communication technology (ICT). This is particularly important in economic, military, and diplomatic responses to cybersecurity threats. Sarwar et al. (2023) supported this view, highlighting the need for national security forces to protect information during exchanges to prevent electronic attacks. By integrating ICT safety protocols, communicators play an active role in reducing cyber risks. Despite extensive research on cybersecurity attitudes, a significant gap remains. There is limited understanding of how communicators' perspectives influence security strategies in national institutions, especially in Kuwait. Addressing this gap is critical for improving cybersecurity communication within national security frameworks.

Moreover, cybersecurity vulnerabilities in small and medium-sized enterprises (SMEs) reveal challenges that may also apply to larger institutions. Ben Romdhane et al. (2025) found that SMEs often face phishing and malware attacks due to limited resources and outdated technologies. Their study recommended employee training and collaboration with cybersecurity specialists to address these gaps. Although focused on SMEs, these findings highlight broader issues such as resource constraints and the need for advanced cybersecurity solutions. National institutions can strengthen their cybersecurity frameworks by implementing similar collaborative approaches. Furthermore, emerging cybersecurity trends require innovative solutions beyond traditional protection systems. Mallick and Nath (2024) noted that firewalls and antivirus software alone are ineffective against sophisticated cyberattacks. They recommended adopting advanced detection techniques and continuously reviewing recent cyberattack patterns to enhance defense mechanisms. This highlights the evolving nature of cybersecurity threats and the importance of keeping communicators informed about new trends. Their role in disseminating information on these advancements is crucial for institutional preparedness. Enhancing communicators' knowledge of advanced cybersecurity strategies can directly improve organizational resilience.

In addition, national and global inconsistencies in cybersecurity policies hinder unified responses to cyber threats. Al Hadeed et al. (2024) analyzed global cybersecurity policies and found significant variations in terminology and transparency across countries. The study recommended developing unified policies and improving evaluation methodologies to address these discrepancies. These findings underscore the need for communicators to advocate for cohesive cybersecurity frameworks within their institutions. Aligning national policies with international standards would enable stronger cybersecurity strategies. Also, technological advancements and geopolitical tensions further complicate cybersecurity challenges in Gulf Cooperation Council (GCC) countries. Haleem Shaikh et al. (2019) highlighted that the energy sector is a major target of cyberattacks in the GCC region. Despite significant investments, securing digital economies remains a challenge. This emphasizes the need for regional cooperation. Communicators play a crucial role in facilitating collaboration among GCC nations to address shared cybersecurity threats. Encouraging cross-border partnerships can strengthen regional cybersecurity resilience, with communicators serving as key facilitators.

Further, national cybersecurity strategies must address local needs while aligning with global standards. Tahat et al. (2023b) examined cybersecurity strategies in the European Union and found significant variations in focus areas. Some countries prioritized protecting critical infrastructure, while others focused on safeguarding personal data. These findings stress the importance of tailoring national strategies to specific contexts while adhering to global best practices. Communicators play a critical role in ensuring these strategies are effectively communicated and implemented. Equipping them with strategic cybersecurity knowledge enhances their ability to align national policies with international standards. Along with these, the rise of cyberwarfare demands integrated strategies and international cooperation. Murad (2023) examined the impact of cyberwarfare on international relations. They noted its borderless nature and rapid escalation. Their study recommended integrated legislation and increased public awareness through education and media campaigns. Communicators play a vital role in raising awareness about cyberwar risks. They bridge the gap between technical experts and the general public. Empowering them with the right tools and knowledge can significantly contribute to national security.

Additionally, cybersecurity legislation and procedural gaps hinder effective responses to cyber threats in many regions. Tahat et al. (2024) found that while cybersecurity systems in Morocco protect institutional data, legislative gaps impede the detection and prosecution of cybercrimes. The study recommended enhancing legal provisions and strengthening international cooperation. These findings are relevant to Kuwaiti institutions, which face similar challenges. Improving legal

awareness among communicators can enhance institutional responses to cyber incidents. Bridging legislative gaps through informed communication strategies can strengthen cybersecurity preparedness in national institutions. Similarly, public awareness campaigns and employee training are critical in reducing cybersecurity risks. Hamzah et al. (2022) found that 65% of Algerian internet users had experienced digital hacks. Their study emphasized the need for stronger public awareness and cybersecurity legislation. They recommended user education and psychological support for victims of cyberattacks. Communicators play a crucial role in designing and implementing effective awareness campaigns. These campaigns can reduce cybersecurity risks and build public trust in digital platforms. By leveraging communicators' expertise, institutions can develop targeted initiatives to address cybersecurity challenges effectively.

Digital hacks also significantly impact Algerian society by undermining trust in digital platforms and exposing critical vulnerabilities. Alhanatleh et al. (2023) conducted a descriptive study involving 1,000 Algerian internet users. Their research found that 65% of participants had experienced cyberattacks such as data theft, financial breaches, and phishing. The study recommended enhancing security awareness, strengthening cybersecurity legislation, and offering psychological and social support to victims. These findings highlight the far-reaching effects of cyberattacks, which erode user confidence in digital systems. This loss of trust underscores the urgency of cybersecurity education and platform security improvements. Addressing these vulnerabilities through targeted education and improved digital security measures is essential for restoring public confidence and enhancing national cybersecurity resilience.

Thus, cybersecurity has fundamentally reshaped international security, necessitating enhanced legal frameworks and global cooperation. Jamal Al-Din (2023) highlighted the growing importance of cybersecurity in international law. His study noted that cyber threats have transformed traditional concepts of security and peace. However, significant legal gaps remain, allowing some states to exploit cyber vulnerabilities without accountability. The study recommended establishing clear international agreements to address these issues. The lack of strong legal frameworks exacerbates cyber risks, enabling malicious actors to exploit weaknesses in international law. These findings highlight the importance of holding states accountable and fostering international cooperation to mitigate cyber threats. Strengthening global cybersecurity laws is critical to ensuring accountability and promoting peace and security.

Similarly, cyberterrorism poses a significant threat to national security, demanding international cooperation and robust countermeasures. For instance, Al Doghmi et al. (2013) used a historical and case study approach to examine the impact of cyberterrorism on Algerian national security. The study emphasized technological advancements as a driving factor behind the rise of cyberterrorism, and highlighted Algeria's need for international collaboration to curb its spread. It shows that cyberterrorism represents a growing threat, exploiting technological progress to destabilize nations. This research demonstrates that no single nation can address this issue independently, necessitating international partnerships and a unified global response. Thus, collaborative international efforts and advanced cybersecurity strategies are essential to counter the escalating threats of cyberterrorism effectively. Additionally, cybersecurity is a critical component of national security, particularly in nations with weak systems. As Al-Shammari (2021) identified weak cybersecurity systems in Iraq as a major vulnerability, enabling terrorist groups to exploit cyberspace and threatening critical infrastructure. The study emphasized cybersecurity's role in enhancing national stability. These findings illustrate the interconnectedness of cybersecurity and national stability, particularly in regions where weak systems invite exploitation. Strengthening cybersecurity is therefore essential for maintaining state security and deterring potential threats. In sum, bolstering national cybersecurity infrastructure is vital to safeguarding critical systems and promoting long-term stability.

So, continuous advancements in technology and the prevalence of cybercrime demand strengthened cybersecurity efforts. Such as, Hamzah et al. (2022) identified significant challenges in combating cybercrime in Algeria due to advancements in information and communication technologies. The study emphasized the need for new legislation, specialized cybersecurity structures, and increased public awareness through education and training programs. As cybercrime becomes more sophisticated, existing measures are insufficient, necessitating innovation in legal and institutional responses. This emphasizes the importance of aligning cybersecurity efforts with technological progress to address emerging threats effectively. Hence, developing adaptive legal and institutional frameworks can enhance national cybersecurity efforts and keep pace with evolving cyber threats.

In this backdrop, penal legislation in GCC countries plays a vital role in addressing cybercrimes but requires legal revisions to mitigate evolving risks. For example, Lee et al. (2023) employed a critical analytical approach to examine penal laws in GCC nations, noting that while various offenses are criminalized, existing laws need revisions to address emerging cyber risks comprehensively. This study highlights the dynamic nature of cybersecurity threats, which often outpace legislative measures. This emphasizes the need for proactive legal updates and harmonization across GCC countries to ensure robust cybersecurity. Thus, revising and harmonizing penal legislation across GCC nations can enhance their capacity to address emerging cyber threats effectively. Also, sophisticated cybercrimes demand innovative strategies and enhanced international cooperation. Such as, Muslim (2021) found that increasingly complex cybercrimes require security institutions to develop novel strategies for detection and prevention. The study emphasized the importance of international cooperation to address these global threats. As cybercrimes transcend borders, collaborative approaches among nations become indispensable. This necessitates a shift from localized efforts to global strategies that leverage shared expertise and resources. Overall, establishing international partnerships and adopting innovative strategies are critical for combating sophisticated cybercrimes effectively.

Importantly, cyberterrorism poses a significant threat to national security, driven by ideological extremism and countered by advanced protection systems. For example, Alnujaifi et al. (2024) conducted a field study on the National Cybersecurity Authority in Saudi Arabia, using a descriptive survey methodology with questionnaires distributed to information security specialists. The study found that ideological extremism is the primary driver of cyberterrorist operations. Organizations in Saudi Arabia rely on highly advanced protection systems to ensure national cybersecurity. The study recommended strengthening technical systems with the latest technologies to combat digital cyberattacks effectively.

These findings highlight the critical role of advanced cybersecurity technologies in mitigating the risks posed by cyberterrorism. However, the reliance on technology alone may not address the broader societal and ideological factors fueling cyberterrorism, underscoring the need for comprehensive strategies that include counter-ideological measures and public awareness campaigns. Hence, strengthening technical systems alongside addressing the ideological roots of cyberterrorism is essential for ensuring national security and safeguarding against evolving cyber threats. In the same way Cybersecurity is integral to achieving national visions like Saudi Arabia's Vision 2030.

Such as, Al-Otaibi (2020) conducted a descriptive study in Saudi Arabia, highlighting significant challenges, including a lack of awareness and expertise among workers, as obstacles to implementing cybersecurity measures in line with Vision 2030. These findings emphasize the importance of aligning cybersecurity efforts with broader national goals. Addressing awareness and training gaps is essential for achieving these ambitions. So, investing in workforce development and targeted awareness initiatives can ensure cybersecurity measures effectively support national strategies.

While the focus on Kuwaiti and GCC-specific studies strengthens the local context, integrating global cybersecurity perspectives provides valuable benchmarks for understanding how national institutions can enhance their cybersecurity frameworks. Nations with mature cybersecurity ecosystems, such as the United States, European Union member states, and Singapore, offer comparative insights that can inform best practices for policy development, institutional preparedness, and incident response in Kuwait.

In this perspective, countries with well-established cybersecurity policies, such as the United States (U. S.) and the European Union (EU), have implemented comprehensive legislative frameworks to address cybersecurity risks effectively. In the U. S., the Cybersecurity and Infrastructure Security Agency (CISA) plays a crucial role in coordinating public-private partnerships to enhance national cybersecurity resilience (Cybersecurity and Infrastructure Security Agency, 2022). Kuwait can adopt a similar approach by expanding the role of CITRA to facilitate greater collaboration between government agencies, media professionals, and private sector stakeholders. While the European Union's General Data Protection Regulation (GDPR) provides a rigorous framework for data privacy and cybersecurity enforcement (European Commission, 2023). Kuwaiti institutions could benefit from adopting similar data protection measures to enhance digital security and compliance with international cybersecurity standards. Similarly, Singapore, a global leader in cybersecurity, has institutionalized cybersecurity through a centralized regulatory body, the Cyber Security Agency (CSA). The CSA implements nationwide public awareness campaigns, workforce training programs, and real-time threat monitoring (Cyber Security Agency of Singapore, 2023). Kuwait's national institutions could adopt Singapore's proactive approach by integrating communicators into cybersecurity planning and real-time crisis response strategies.

Moreover, in the U. S., federal agencies regularly conduct cybersecurity drills and simulations to test institutional readiness against cyberattacks. For instance, Cyber Storm, a biennial cybersecurity exercise conducted by CISA, evaluates national resilience in responding to cyber incidents (Department of Homeland Security, 2023). Kuwait could implement similar large-scale cybersecurity simulations, ensuring national institutions are prepared to handle cyber threats effectively. On the other hand, Japan has emphasized cybersecurity workforce development by integrating cybersecurity education into higher education curricula and government training programs (National Institute of Information and Communications Technology, 2022). Kuwaiti universities and research institutions could adopt this model to train communicators in cybersecurity crisis management, enhancing their role in cybersecurity awareness campaigns. While the UK's National Cyber Security Centre (NCSC) has pioneered cybersecurity information-sharing frameworks that connect government agencies, businesses, and media organizations to ensure a unified response to cyber threats (National Cyber Security Centre, 2023). In the same way, establishing a Kuwaiti equivalent of the NCSC could streamline cybersecurity communications and enable more effective public outreach efforts.

In addition, countries with advanced cybersecurity cultures prioritize continuous public engagement. For example, Estonia, widely regarded as a global leader in digital governance, has integrated cybersecurity training into school curricula, ensuring that even young citizens develop cyber awareness from an early age (e-Governance Academy, 2023). Kuwait could benefit from implementing cybersecurity education programs in schools, universities, and public-sector training initiatives to build a long-term cybersecurity-aware culture. While South Korea has implemented mandatory cybersecurity certifications for media professionals working in state institutions to ensure accurate cybersecurity reporting and crisis communication. A similar certification system could be introduced in Kuwait to enhance the cybersecurity competency of communicators in national institutions. Thus, integrating global best practices with Kuwait's existing cybersecurity policies will enable national institutions to build a more resilient cybersecurity ecosystem. The lessons from technologically advanced nations emphasize the need for proactive policy enforcement, cybersecurity training, public-private partnerships, and institutional preparedness strategies. By adopting and adapting these international benchmarks, Kuwait can strengthen its cybersecurity frameworks while maintaining cultural and institutional relevance.

In general, the existing literature highlights significant advancements in understanding cybersecurity challenges and practices across various sectors. For instance, Dawson (2018) underscores the growing complexity of cyber threats and emphasizes the need for multidisciplinary approaches, including strategic communication, to address these challenges. Similarly, Mansoori et al. (2024) explored the integration of communication strategies with technological measures to mitigate cyber risks. However, while these studies focus broadly on cybersecurity strategies, their relevance to communicators' attitudes and practices within national institutions remains underexplored. This study aims to bridge this gap by focusing specifically on how communicators in Kuwaiti national institutions perceive and respond to cybersecurity issues.

Despite a growing body of research on cybersecurity, gaps persist in understanding the specific role of communicators in national institutions. Prior studies, such as those by Han and Zhang (2020) and Mallick and Nath (2024), discuss cybersecurity measures and their effectiveness; but fail to examine the attitudes and behaviors of communicators who serve as critical links between technical experts and institutional leadership. Additionally, studies conducted in the Arab region, such as those by Khader et al. (2021) and Tahat and Al-Mutairi (2022), focus on

legislative frameworks and technical solutions without exploring how communicators' awareness and attitudes influence cybersecurity practices. This study addresses these gaps by investigating communicators' perspectives, their preparedness to tackle cyber threats, and their role in shaping institutional responses to cybersecurity challenges. Hence, this study aligns with previous research, such as Tabassum and Baker (2020), which emphasizes the importance of raising cybersecurity awareness through education and training. However, by focusing on communicators in national institutions, it seeks to expand on this work by identifying the specific factors influencing their attitudes and the effectiveness of their communication strategies.

Hence, this study builds upon existing research by addressing a gap in cybersecurity communication, particularly in the Kuwaiti context. While prior studies have examined cybersecurity threats, legislative frameworks, and risk mitigation strategies, limited attention has been given to the role of communicators in shaping cybersecurity awareness and responses. By investigating communicators' cybersecurity attitudes, this study contributes to both academic literature and policy discussions, offering empirical insights that inform cybersecurity preparedness strategies within national institutions. To better understand communicators' adoption of cybersecurity measures, this study is grounded in the Technology Acceptance Model (TAM). The next section outlines this theoretical framework, explaining its relevance in examining communicators' perceptions, ease of use, and behavioral intentions regarding cybersecurity technologies.

Methods and hypotheses

Theoretical framework: technology acceptance model (TAM)

The Technology Acceptance Model (TAM) provides a theoretical foundation for understanding how users adopt and engage with technology (Venkatesh et al., 2000). It has been widely applied in various fields and has received strong empirical support (Tarhini et al., 2016). According to TAM, perceived ease of use (PEU) refers to the extent to which a person believes that using a technological system requires minimal effort. When individuals perceive a system as easy to use, they are more likely to integrate it into their workflow, leading to improved performance outcomes (Davis, 1989). While perceived usefulness (PU) is defined as the degree to which an individual believes that a system will enhance their job performance (Davis, 1989). Similarly, perceived ease of use (PEU) represents the belief that using a particular system will be effortless (Venkatesh et al., 2000). In the context of this study, TAM is used to examine communicators' attitudes toward cybersecurity technologies. PU reflects communicators' belief that adopting cybersecurity measures, such as spam regulations and emergency response systems, will enhance their effectiveness. PEU represents their perception of the effort required to implement these measures successfully. Similarly, behavioral intention (BI) serves as an intermediary variable, influenced by PU and PEU, in predicting the likelihood of communicators adopting cybersecurity practices. The hypotheses in this study are aligned with these constructs to ensure a clear integration of theory and study variables.

The hypotheses were developed based on TAM and a review of existing literature on cybersecurity legislation, institutional cybersecurity practices, and communicators' roles in national security frameworks. This study investigates communicators' cybersecurity attitudes in Kuwaiti national institutions, integrating PU, PEU, and BI as core constructs influencing their cybersecurity engagement. The proposed research model categorizes three key variables that may influence behavioral intentions (BI) and actual use (AU). These categories provide a structured approach to understanding communicators' acceptance of cybersecurity measures (Dumpit and Fernandez, 2017; Lederer et al., 2000; Tarhini et al., 2016).

Hypotheses

> *H1*: There is a significant statistical relationship between the enforcement of legislation and laws and the level of response to cybersecurity threats in national institutions.

Perceived usefulness (PU) significantly impacts behavioral intention (BI) (Davis, 1989; Venkatesh et al., 2000). Cybersecurity policies and legal frameworks serve as institutional enablers, shaping the extent to which communicators perceive cybersecurity measures as beneficial to their work. Prior research suggests that strong legislative enforcement leads to higher compliance with security protocols (Tarhini et al., 2016; Dawson et al., 2023). Greater enforcement of cybersecurity laws is expected to positively influence the responsiveness of national institutions to cyber threats.

> *H2*: There is a significant statistical relationship between the presence of legislation and laws and their effective implementation by responsible personnel in national institutions.

The implementation of cybersecurity legislation depends not only on legal provisions but also on institutional adherence (Khader et al., 2021). Research in digital governance highlights that when laws are clear and well-enforced, responsible personnel are more likely to comply with cybersecurity measures (Han and Zhang, 2020). A strong legal framework is expected to correlate directly with its practical enforcement by professionals within national institutions.

> *H3*: There is a significant statistical relationship between curbing spam messages and the communicator's ability to respond to cyber incident threats in national institutions.

Phishing and spam messages are among the most common entry points for cyberattacks, targeting institutional vulnerabilities (Dawson et al., 2023). Effective cybersecurity communication ensures that personnel recognize and respond appropriately to such threats (Sharma and Maurya, 2020). The ability to curb spam messages is expected to enhance communicators' responsiveness to cybersecurity incidents, aligning with previous studies on cybersecurity awareness and response efficiency (Mijwil et al., 2023).

> *H4*: There is a significant statistical relationship between the plans and methods used to address cybersecurity threats and the existence of procedural laws or legislation governing cybercrimes among communicators in national institutions.

Effective cybersecurity response strategies require technical readiness and institutional alignment with procedural laws (Tahat and Al-Mutairi, 2022). Studies indicate that when communicators are equipped with structured response frameworks, institutional cybersecurity preparedness improves (Murad, 2023). If cybersecurity plans and methods are well-structured and legally backed, communicators are expected to be more engaged in security efforts.

Each hypothesis is designed to align with these constructs, ensuring a coherent integration of theory and study variables. After establishing a theoretical framework that guides this study, the next section outlines the procedures and methodology (Figure 1).

Procedures and methodology

The following section details the research design, data collection methods, and statistical analysis techniques used to examine communicators' attitudes toward cybersecurity in Kuwaiti national institutions. The methodology in scientific research is the cornerstone of any study, serving as the pathway to uncovering the research problem and achieving its objectives (Habes et al., 2024; Mansoori et al., 2024; Tahat et al., 2024; Attar et al., 2024; Elareshi et al., 2024; Tahat et al., 2023a; Tahat et al., 2023b). The nature of current study and research questions primarily focus on the attitudes of communicators toward cybersecurity in ensuring safety and security within national institutions. The study employs a quantitative descriptive approach, supported by rigorous statistical methods (Habes et al., 2021, 2023). Control variables were carefully selected to account for potential confounding effects that might influence the relationships between cybersecurity legislation, communicators' attitudes, and their adoption of security practices. The selection process was guided by theoretical frameworks, primarily the TAM, and empirical evidence from previous studies on cybersecurity behavior and institutional adoption of security measures. The final control variables, including age, gender, educational level, and years of experience, were chosen based on their well-documented influence on technology acceptance, cybersecurity awareness, and institutional compliance (Davis, 1989; Venkatesh et al., 2003; Tarhini et al., 2016).

Moreover, during the initial conceptualization of the study, several additional control variables were investigated based on prior research and preliminary statistical analysis. However, these variables were later excluded from the final analysis due to statistical insignificance, conceptual redundancy, or data limitations. The decision to remove these variables was guided by empirical testing to ensure that only meaningful and non-redundant predictors were included in the final model. These initially included variables were; institution type (public vs. private national institutions), position level (entry-level vs. senior-level communicators), frequency of cybersecurity training, and departmental role (IT vs. non-IT communicators).

The selection and recruitment of participants were conducted systematically to ensure that the sample accurately reflected communicators working in Kuwaiti national institutions. The target population included professional communicators from government agencies, public sector organizations, and regulatory bodies. To ensure that participants had direct experience with institutional cybersecurity practices, inclusion criteria were established. Eligible participants were required to have at least 1 year of experience in communication roles within national institutions, be responsible for cybersecurity awareness, media communication, or policy dissemination, and be actively engaged in institutional cybersecurity discussions, training, or response efforts.

A convenience sampling approach was employed to recruit participants. While probability sampling is ideal for ensuring generalizability, it was not feasible in this study due to limited access to cybersecurity communicators in government institutions. Convenience sampling was chosen as it allowed for efficient recruitment of professionals actively involved in cybersecurity communication, facilitated access to participants who were willing

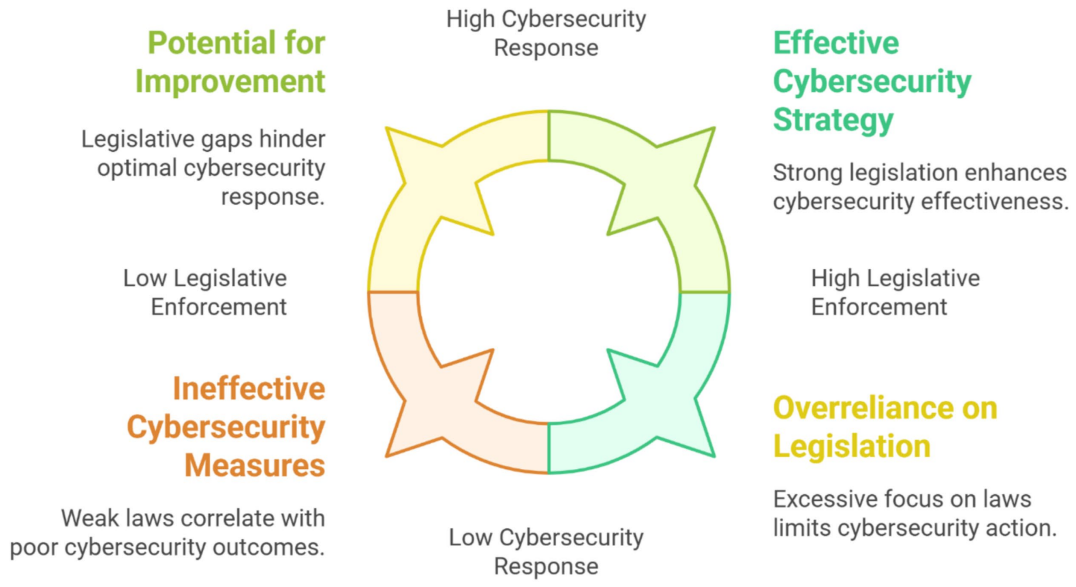

FIGURE 1
Impact of legislation on cybersecurity response.

and available to participate despite institutional restrictions on research participation, and aligned with previous studies on cybersecurity professionals, where similar non-random sampling strategies were successfully employed due to restricted participant availability (Etikan et al., 2016).

The recruitment process followed an ethical and structured approach to ensure participant willingness and confidentiality. Before recruitment, formal approvals were sought from relevant governmental authorities and institutional review boards to ensure compliance with research ethics. A letter detailing the research purpose and confidentiality measures was provided to potential participants. Potential participants were identified through government institutions and professional networks, and invitations were sent via official emails and internal communication channels, outlining the study objectives and voluntary participation guidelines. Prior to participation, all respondents provided informed consent, acknowledging their rights, the study's purpose, and data confidentiality. To protect anonymity, no personal identifiers were collected, and responses were securely stored. A pilot recruitment phase was conducted with a subset of 20 communicators to assess the feasibility of the recruitment strategy and refine the selection approach. Feedback was collected to ensure that the recruitment strategy aligned with institutional policies and participant expectations, further enhancing the reliability of the participant selection process. A total of 140 communicators participated in the study, which was deemed sufficient for statistical analysis and hypothesis testing. This sample size ensured adequate representation of communicators from different national institutions. The size determination was based on prior studies on cybersecurity attitudes, where similar sample sizes yielded valid results (Dawson et al., 2023).

As this study focused on communicators in Kuwaiti national institutions involved in public communication, cybersecurity awareness, policy dissemination, and institutional security measures. Targeted organizations included government ministries, security agencies, regulatory bodies, government-owned corporations, and academic institutions, all selected for their direct role in national cybersecurity strategies. Key institutions included the Ministry of Interior, Ministry of Information, CITRA, Ministry of Finance, Kuwait National Security Bureau, Cybercrime Combatting Unit, Kuwait Petroleum Corporation, CAIT, Kuwait University, and PAAET. Participants were institutional communicators, cybersecurity policy experts, media officers, and a limited number of IT security professionals, all engaged in cybersecurity awareness, policy enforcement, or public communication. Inclusion criteria required at least 1 year of experience in cybersecurity-related communication and familiarity with cybersecurity laws in Kuwait. Among 140 professionals, 58% (81 participants) were from government ministries and regulatory agencies, 23% (32 participants) from law enforcement and security organizations, 12% (17 participants) from government-owned corporations and cybersecurity institutions, and 7% (10 participants) from academic and research institutions.

While convenient sampling method facilitated practical and efficient data collection, it introduced potential biases, such as limited representation across all sectors. These biases restrict the generalizability of findings beyond the sampled population. To address these limitations, the sample size was set at 140 respondents, ensuring adequacy for statistical analysis, and efforts were made to include participants with diverse demographic characteristics, including age, gender, and institutional affiliations. More critically, the use of convenience sampling in this study was a practical and necessary choice, given the challenges of accessing cybersecurity communicators in Kuwaiti national institutions. This method allowed for an efficient collection of data from professionals actively engaged in cybersecurity communication. However, it is acknowledged that convenience sampling has inherent limitations that may affect the generalizability of the findings (Etikan et al., 2016). One of the primary concerns with convenience sampling is selection bias, as participants are drawn from readily available groups rather than randomly selected from the entire population (Bornstein et al., 2013). This can lead to an overrepresentation or underrepresentation of certain demographic or professional groups, potentially influencing the study's outcomes.

In the context of this research, the sample was predominantly male (77.1%), and the majority held a bachelor's degree (72.1%), which may not fully reflect the diversity of cybersecurity communicators in Kuwait. Moreover, convenience sampling limits the external validity of the study, meaning that the findings may not be directly applicable to other national institutions or countries with different cybersecurity policies and communication structures (Jager et al., 2017). While the insights gained provide valuable knowledge on communicators' attitudes within Kuwaiti institutions, caution should be exercised when applying these conclusions to broader contexts.

To mitigate these limitations, future research should consider employing probability sampling methods, such as stratified random sampling, to ensure a more representative sample of communicators across various institutions and experience levels (Taherdoost, 2018). Additionally, mixed-methods approaches integrating qualitative interviews with key stakeholders could provide deeper insights and strengthen the study's applicability. Despite these limitations, the study's methodological rigor was enhanced through a carefully designed questionnaire, pilot testing, and expert validation to ensure reliability and construct validity. The use of statistical controls and comparative analysis further minimized biases, allowing for meaningful interpretations of cybersecurity communicators' attitudes.

Along with these, a questionnaire was developed based on the TAM and relevant constructs: perceived usefulness and ease of use (Davis, 1989; Venkatesh et al., 2000). Each item was designed to capture attitudes and behaviors related to cybersecurity communicators' practices, grounded in the theoretical premises of TAM. Then, the instrument underwent pilot testing with a subset of 20 communicators in national institutions to ensure clarity and relevance (Musallam, 2021). Feedback was used to refine questions for improved comprehension and alignment with the study objectives. In addition, a panel of five experts specializing in cybersecurity communication and quantitative research reviewed the questionnaire for content validity, ensuring that each item effectively captured the intended constructs. Then, questionnaire was distributed to a sample of 140 cybersecurity personnel working in Kuwaiti security institutions (Al Olaimat et al., 2022) (Figure 2).

Instrument reliability: Cronbach's alpha (α)

Importantly, the researchers assessed the reliability of the study instrument for its intended purpose by calculating the Cronbach's Alpha coefficient, which is considered one of the most prominent measures for evaluating the internal consistency of a study instrument. The results

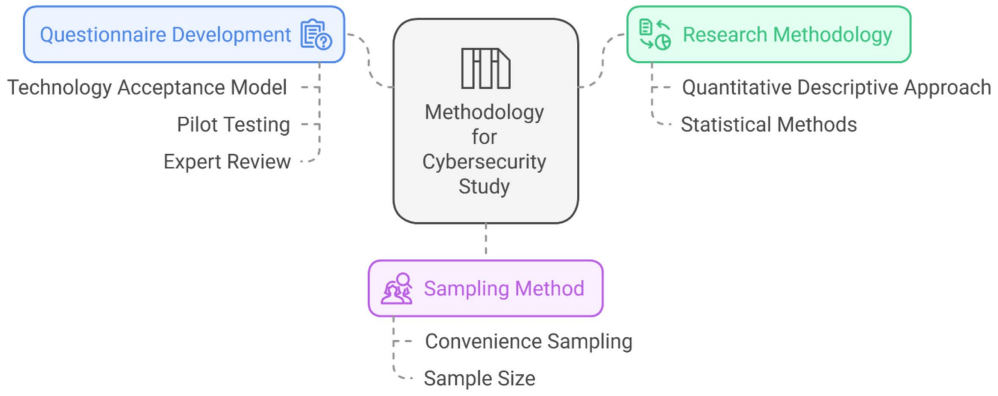

FIGURE 2
Methodology for the study.

indicated that the overall reliability coefficient reached 0.927, which is a very high value. This demonstrates a high level of internal consistency for the study instrument, indicating a significant degree of reliability and its suitability for conducting the study. Moreover, for the construct validity exploratory factor analysis (EFA) was performed to confirm the underlying dimensions of the questionnaire. The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was 0.821, and Bartlett's test of sphericity was significant ($p < 0.001$), confirming the suitability of the data for factor analysis. The content validity index (CVI) for the questionnaire items was 0.88, indicating a high level of agreement among the expert panel regarding the relevance of the questions.

Table 1 Shows the Cronbach's alpha value for each domain of the study.

TABLE 1 Cronbach's alpha value.

Variables	Cronbach's alpha value
Aspects covered by cybercrime laws and legislation	0.730
Laws or legislation related to computer data	0.738
General powers under the Cybercrime Law	0.853
Cybersecurity strategy	0.780
Efforts made to develop cybersecurity	0.872
Institutions most targeted by cybercrime	0.587
Duties of those responsible for cybersecurity in institutions	0.938
Total	0.927

Exclusion of incomplete responses

To ensure data accuracy and reliability, a systematic data cleaning process was conducted. Initially, 161 responses were collected. Incomplete responses exceeding 30% missing data were excluded (9 cases, 6.4%), as they could bias statistical findings (Etikan et al., 2016). Straight-lining responses were removed (5 cases, 3.6%) due to lack of engagement (Dawson et al., 2023). Surveys completed in under 2 min were excluded (4 cases, 2.9%) as genuine responses required 7–10 min. Additionally, 3 cases (2.1%) were removed as they did not meet the inclusion criteria. After excluding 21 cases (13.0%), the final dataset consisted of 140 valid responses, for statistical analysis (Venkatesh et al., 2003).

Defining and handling outliers

Outliers were systematically identified and managed to ensure data reliability and validity while minimizing statistical distortions. A data point was considered an outlier if it deviated beyond ±3 standard deviations from the mean in continuous variables or exceeded 1.5 times the interquartile range (IQR). Additionally, responses displaying unrealistic patterns, such as selecting both "Strongly Agree" and "Strongly Disagree" in logically dependent questions, were flagged for review. Outliers were detected using Z-scores greater than ±3.0, boxplot and histogram analysis, and Mahalanobis distance for identifying multivariate outliers once identified, outliers were handled based on their nature. Valid but extreme responses were retained to preserve genuine variations in cybersecurity attitudes, while Winsorization was applied to adjust extreme values without distorting data trends. However, statistically extreme and conceptually unjustifiable cases were removed, leading to the exclusion of 7 cases (5.0% of the dataset) to prevent misleading conclusions. After outlier management, Kolmogorov–Smirnov and Shapiro–Wilk normality tests, along with skewness/kurtosis evaluations, were conducted to confirm that the data distribution remained stable and methodologically sound.

Hence, these methods ensured that the study findings were both statistically reliable and relevant to the research objectives.

Results and discussion

With the methodology established, the following section presents the results of the study, highlighting key findings related to cybersecurity awareness, institutional preparedness, and communicators' roles in addressing cyber threats.

Here, Table 2 provides a description of the sample based on their demographic characteristics.

Table 2 and Figure 3 indicate that the majority of the study sample were males, with 108 individuals, representing approximately 77.1% of

the total sample. In comparison, 32 females made up about 22.9% of the sample. The use of convenience sampling in this study limits its representativeness, as noted in the previous section. This limitation is particularly evident due to the gender imbalance (77% male) and potential age-related biases. Future research should consider using stratified sampling to ensure proportional representation across key demographic groups. This approach would enhance the validity and generalizability of the findings (Taherdoost, 2018). However, the current study justifies its sampling method, given its exploratory nature and limited access to communicators in Kuwaiti national institutions. This opens opportunities for future studies to address these limitations.

The gender imbalance may also be explained by the fact that more males are working in the field of cybersecurity in Kuwait than females. Regarding age groups, the sample size varied, with relatively close percentages, as shown in Figure 4. Forty-six individuals, or 33% of the sample, were under 30 years old. Those aged 30–39 accounted for about 29%. The remaining participants were distributed between individuals aged 40–49 and those over 50.

The Table 2 and Figure 5 results also indicate that the majority of the sample held a bachelor's degree, with their number reaching 101, accounting for 72%, while the remainder were holders of postgraduate degrees, totaling 39 individuals, or about 28%.

To ensure statistical transparency and methodological rigor, the selected control variables-age, gender, educational level, and years of experience-are included in the correlation matrix alongside independent and dependent variables. This inclusion provides a comprehensive view of how these factors interact with key study variables such as perceived usefulness (PU), perceived ease of use (PEU), and behavioral intention (BI). By incorporating these control variables, the study allows for a clearer assessment of their influence on cybersecurity engagement and the adoption of security measures. This approach ensures that any potential confounding effects are visible and accounted for in subsequent statistical analyses.

Additionally, including control variables in the correlation table aids in identifying potential multicollinearity issues, particularly when variables such as years of experience and educational level may exhibit high correlations with independent variables. This step preserves the integrity of regression analyses by ensuring that none of the variables in the model excessively overlap. Furthermore, the inclusion of control variables enhances the transparency of data reporting, allowing researchers and readers to assess the strength and direction of each control variable's relationship with the primary study constructs.

TABLE 2 Demographic variables.

Variables	Categories	Frequency	Percentage
Sex	Male	108	77.1%
	Female	32	22.9%
Age	Less than 30	46	32.9%
	From 30–39	40	28.6%
	From 40–49	23	16.4%
	50 and above	31	22.1%
Academic degree	Bachelor	101	72.1%
	Postgraduate studies	39	27.9%
Total		140	100

The correlation Table 3 below presents all variable relationships openly, reinforcing the study's commitment to full disclosure and statistical transparency. The significance indicators (*p-values*) highlight relationships that are statistically meaningful.

Domain one: The existence of laws or legislation related to cybercrimes

Table 4 presents the responses of participants regarding the existence of laws or legislation related to cybercrimes. The high agreement rate (88.6%) indicates a strong acknowledgment of legal frameworks. However, the 11.4% disagreement highlights a minority perception of gaps in enforcement or awareness. This contrast underscores the need for targeted legal literacy programs to ensure comprehensive understanding among communicators. Also, these results indicate that most respondents acknowledged the presence of laws and regulations related to cybersecurity in Kuwaiti national institutions. A total of 124 participants, representing approximately 89% of the sample, confirmed the existence of such regulations. In contrast, only 16 respondents, or 11%, reported the absence of cybersecurity laws. This finding highlights Kuwait's strong commitment to regulating cybersecurity within institutions. The presence of these laws serves as a crucial deterrent against potential cyber threats.

This result aligns with the study by Al-Jenfawi (2023) which confirmed the existence of cybersecurity regulations in Kuwaiti institutions. It also emphasized their continuous development to meet the demands of digital transformation. Similarly, Khan and Ahmed, (2024) found that Egypt has implemented legislative and regulatory frameworks to protect against cybersecurity threats. These measures aim to safeguard digital security and mitigate risks associated with cyberattacks. Since this study focuses on cybersecurity communicators, respondents who reported the absence of cybersecurity laws were excluded from further participation. As a result, the final sample for statistical analysis consisted of 124 valid questionnaires.

On the other hand, although Kuwait has established a legal framework for cybersecurity through CITRA, yet its effectiveness is constrained by several implementation challenges. The limited awareness of legal responsibilities among institutions, combined with inadequate enforcement mechanisms, reduces compliance and leaves critical gaps (Mijwil et al., 2023). Furthermore, the rapidly evolving nature of cyber threats, such as ransomware and deepfakes, highlights the need for periodic updates to the legal framework. In comparison, nations like Singapore and the UAE demonstrate the benefits of proactive legal adaptation and international cooperation in addressing cyber risks (Mallick and Nath, 2024). Kuwait can enhance its cybersecurity laws by aligning with international standards, increasing training for enforcement personnel, and fostering global partnerships.

Domain two: Procedural laws or legislation for cybercrimes

Table 5 give detailed responses on procedural laws for cybercrimes. Notably, 57.1% of participants affirmed the existence of confidentiality regulations, the highest agreement level among procedural laws. Conversely, only 40% recognized provisions for real-time data collection,

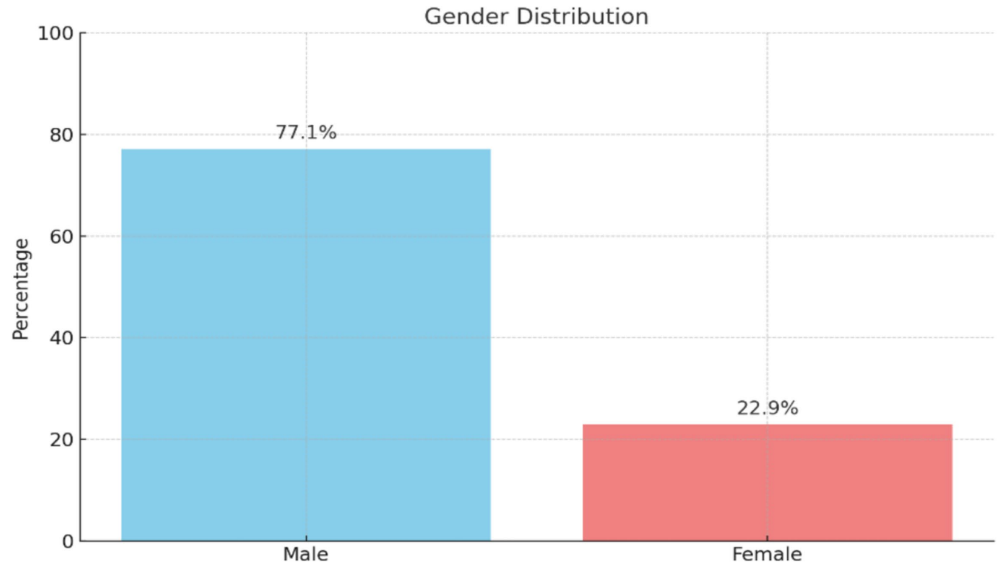

FIGURE 3
Gender distribution of the participants.

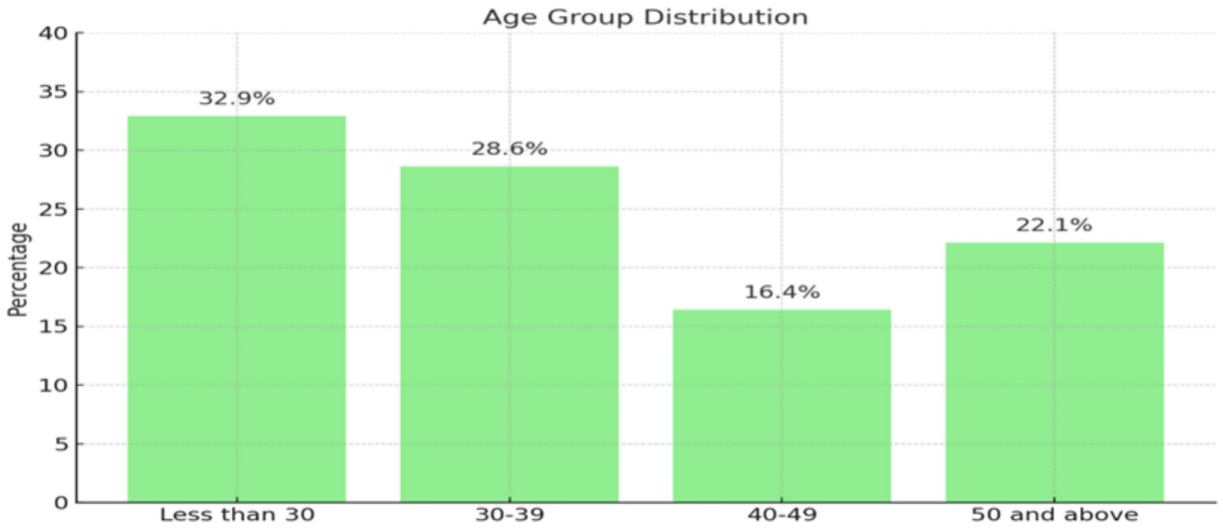

FIGURE 4
Age distribution of the participants.

indicating a potential gap in legal awareness. These findings emphasize the importance of educating communicators on procedural legislation.

Similarly, Figure 6 illustrates participants' awareness of procedural laws for cybercrimes. Notably, 57.1% confirmed the presence of confidentiality laws, reflecting strong awareness of data protection measures. However, the comparatively low 40% recognition of real-time data collection provisions indicates a gap in knowledge of technical surveillance laws. This disparity highlights the need for targeted legal training programs within national institutions.

More explicitly, the results in Table 5 and Figure 6 reveal that most of the sample agreed on the existence of several procedural laws and legislation related to cybersecurity. One such article, related to "confidentiality or restricting use," recorded the lowest mean score of 1.40 and the smallest standard deviation of 0.48. This suggests inconsistency in the respondents' answers. Nevertheless, more than half of the sample-80 individuals, or 57%-confirmed the presence of this article in the law. Only 6 individuals reported its absence. Similarly, the article on "extradition of cybercriminals" obtained a mean score of 1.49 and a standard deviation of 0.68, indicating variability in responses. A total of 76 participants (54.3%) confirmed the existence of this article, while 13 respondents (9%) indicated that it does not exist.

Regarding the article on the "quick preservation of stored computer data," the results were more consistent. It received the highest mean score of 1.65, with a standard deviation of 0.69. Forty-two percent of the sample, or 59 individuals, confirmed the presence of this article, while only 11% (16 respondents) denied its

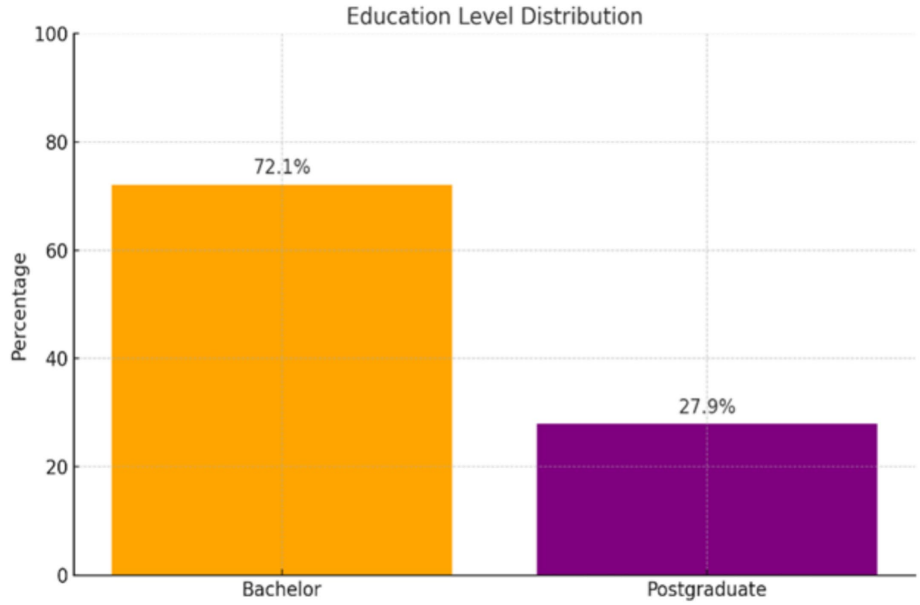

FIGURE 5
Education level distribution of the participants.

TABLE 3 Correlation of control variables.

Variables	1	2	3	4	5	6	7	8
1. Age	1							
2. Gender	0.12	1						
3. Educational level	−0.08	0.15*	1					
4. Years of experience	0.42**	0.09	0.33**	1				
5. Perceived usefulness (PU)	0.25*	0.05	0.28**	0.39**	1			
6. Perceived ease of use (PEU)	0.18	−0.02	0.21*	0.29**	0.52**	1		
7. Behavioral intention (BI)	0.31**	0.07	0.26*	0.41**	0.61**	0.48**	1	
8. Cybersecurity engagement	0.20*	0.06	0.24*	0.36**	0.55**	0.43**	0.58**	1

*$p < 0.05$, **$p < 0.01$.

existence. Additionally, 35% (49 respondents) stated that they were unsure whether it exists. The mean and standard deviation for the other articles showed relatively similar results, with a narrow range of 2. This indicates that respondents held similar views on these articles, and the variance in their responses was minimal, with no significant differences between the lowest and highest values.

TABLE 4 Existence of laws or legislation related to cybercrimes.

Are there laws or legislation related to cybercrime?	Frequencies	Percentage
Yes	124	88.6%
No	16	11.4%

Domain three: The existence of laws or legislation related to curbing spam messages

Table 6 shows varying opinions on laws curbing spam messages, with only 29.3% affirming their existence. The high neutrality (26.4%) suggests uncertainty or limited knowledge, while the 32.9% disagreement indicates skepticism about enforcement. These results point to a gap in awareness campaigns, warranting clearer communication strategies. The mean score was 2.04, indicating a clear divergence in participants' opinions. The standard deviation was 0.84, suggesting a lack of consensus among the sample and noticeable differences in their views. These differences are particularly evident in the responses regarding laws or regulations related to curbing spam messages. Although the sample variations appear small, and have mixed responses (29.3% agreement, 26.4% neutrality, 32.9% disagreement), a chi-square test for independence was conducted to assess statistical significance, yielding χ^2 (2, $N = 124$) = 7.21, $p = 0.027$, indicating a significant association. The high neutrality rate (26.4%) suggests a gap in awareness, highlighting the need for clearer institutional communication about anti-spam legislation. While, the significant association ($p = 0.027$) suggests institutional outreach

TABLE 5 Procedural laws and legislation for cybercrimes.

Procedural laws or legislation for cybercrimes		Frequencies	Percentage	Mean	Standard deviation	Range
Materials on quick preservation of stored computer data	Agree	59	42.1%	1.65	0.69	2
	Neutral	49	35%			
	Disagree	16	11.4%			
Materials regarding disclosure orders	Agree	58	41.4%	1.62	0.65	2
	Neutral	54	38.6%			
	Disagree	12	8.6%			
Materials regarding searching and preserving stored computer data	Agree	64	45.7%	1.62	0.72	2
	Neutral	42	30%			
	Disagree	18	12.9%			
Materials related to real-time computer data collection	Agree	56	40%	1.63	0.64	2
	Neutral	57	40.7%			
	Disagree	11	7.9%			
Materials relating to the extradition of cybercriminals	Agree	76	54.3%	1.49	0.68	2
	Neutral	35	25%			
	Disagree	13	9.3%			
Materials related to mutual assistance	Agree	65	46.4%	1.54	0.629	2
	Neutral	50	35.7%			
	Disagree	9	6.4%			
Materials relating to confidentiality or restriction of use	Agree	80	57.1%	1.40	0.48	2
	Neutral	38	27.1%			
	Disagree	6	4.3%			

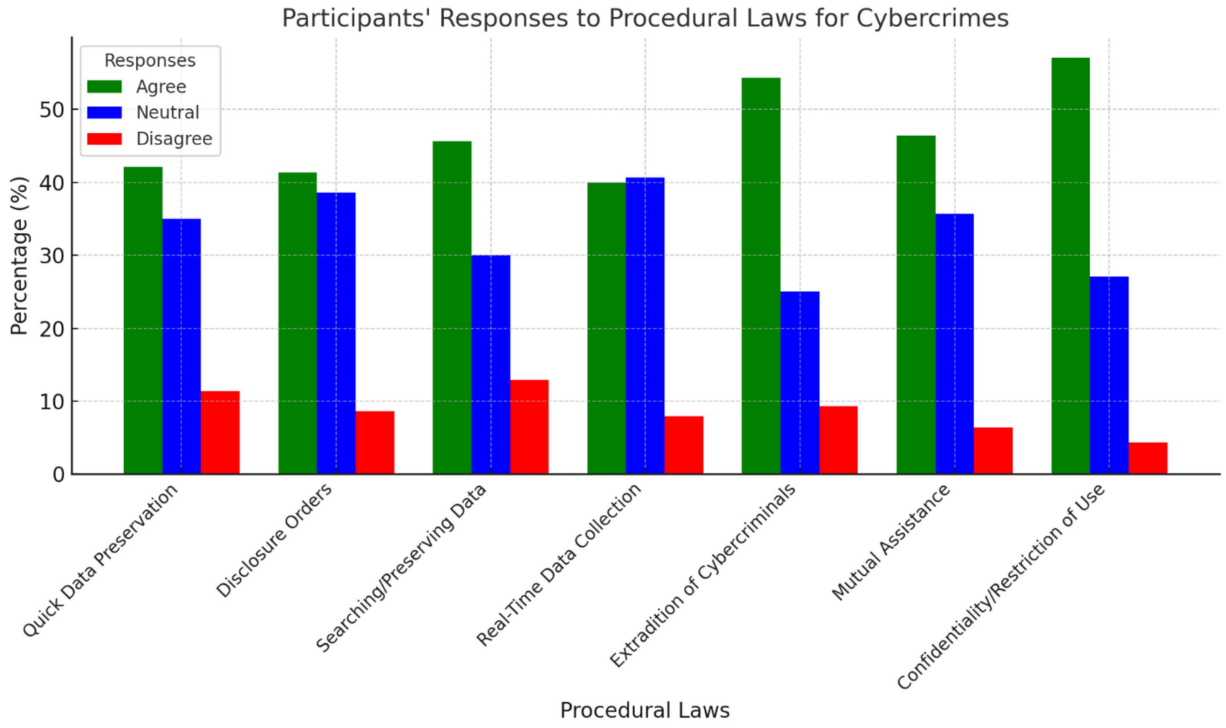

FIGURE 6
Participants response to procedural laws for cybercrimes.

efforts could directly influence participants' understanding and opinions.

Domain four: How to respond to cyber incident threats and measurement standards

The results in Table 7 and Figure 7 show that the presence of a Computer Emergency Response Team (CERT) received the lowest mean value of 1.78 and the lowest standard deviation of 0.79. The low variance can be explained by the number of respondents who confirmed the existence of such teams in their organizations. A total of 55 individuals, or approximately 39% of the sample, affirmed the presence of CERT teams. In contrast, 28 individuals (23%) did not confirm their existence. Meanwhile, 41 respondents (33%) lacked sufficient awareness of the matter. These differences in responses indicate that participants were more likely to agree on the existence of CERT teams. The results also show a similarity in mean values between the presence of a Security Incident Response Team (1.87) and a Computer Incident Response Team (1.88). The consistency in their standard deviations suggests that opinions on computer-related incidents are similar to those on security-related incidents.

From these findings, it is clear that there are knowledge gaps among participants regarding the existence of such teams in their organizations, especially in relation to computer and security incidents. This study highlights a significant knowledge gap regarding the roles of CERT teams among communicators in Kuwaiti national institutions. Specifically, 33.1% of participants reported neutrality, while 28.2% disagreed about the presence of CERT teams.

This lack of awareness may stem from limited internal communication, inadequate training, and organizational silos between cybersecurity and communication teams. This gap has critical implications for institutional cybersecurity, as uninformed communicators may unintentionally hinder incident response efforts. To address this, institutions should prioritize training programs, promote cross-departmental collaboration, and increase the visibility of CERT teams. Such measures are consistent with best practices identified in recent research, which emphasizes the importance of integrating technical expertise with strategic communication to enhance overall cybersecurity resilience (Mijwil et al., 2023; Mallick and Nath, 2024).

Domain five: Plans and approaches followed by the communicator regarding cybersecurity threats

Figure 8 highlights the varied methods communicators employ in addressing cybersecurity threats. Social media campaigns received the highest agreement (57.3%), indicating a preference for digital outreach. Conversely, expert meetings with students (33.9%) ranked lowest, suggesting limited outreach initiatives in educational contexts. These findings emphasize the importance of diversifying awareness strategies, including expanding outreach to schools and universities.

Collectively, the results in Table 8 and Figure 8 show variations in the plans and methods communicators use to address cybersecurity threats. The most notable method was using social media for cybersecurity awareness, which received the lowest mean score of 1.56 and a standard deviation of 0.72. This indicates moderate variance, as participants showed limited agreement on this method. More than half of the sample (57%, or 71 individuals) confirmed it as one of the

TABLE 6 The existence of laws or legislation related to curbing spam messages.

The existence of laws or legislation related to curbing spam messages	Frequencies	Percentage	Mean	Standard deviation	Range
Agree	41	29.3%	2.04	0.84	2
Neutral					
Disagree	37	26.4%			
	46	32.9%			

TABLE 7 How to respond to cyber incident threats.

How to respond to cyber incident threats		Frequencies	Percentage	Mean	Standard deviation	Range
Presence of a computer incident response team	Agree	49	39.5%	1.88	0.81	2
	Neutral	40	32.3%			
	Disagree	35	28.2%			
Having a team to respond to security incidents	Agree	49	39.5%	1.87	0.80	2
	Neutral	42	33.9%			
	Disagree	33	26.6%			
Having a computer emergency response team	Agree	55	44.4%	1.78	0.79	2
	Neutral	41	33.1%			
	Disagree	28	22.6%			

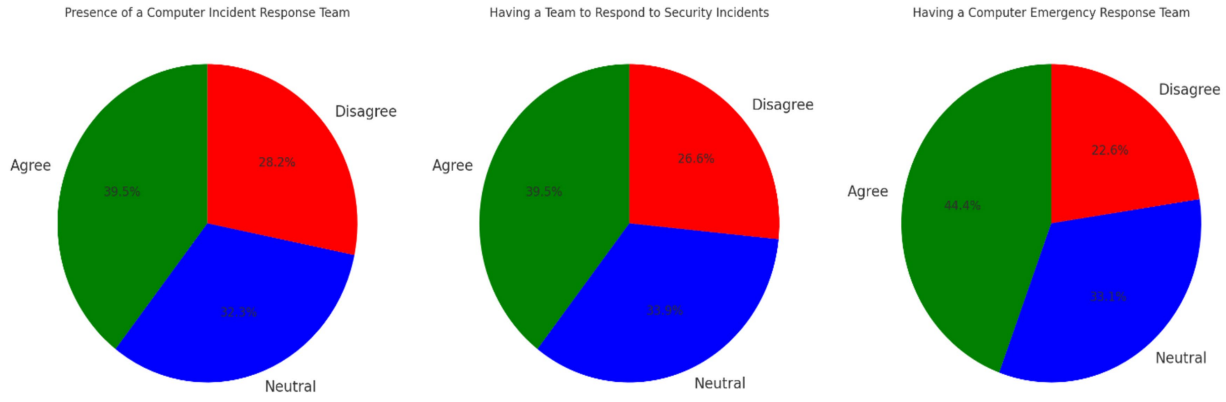

FIGURE 7
Respond to Cyber Incident Threats.

methods. However, 13% (17 participants) disagreed, and 26% (36 individuals) lacked sufficient knowledge on the topic.

Next, awareness lectures and seminars on cybersecurity had a mean score of 1.60 and a standard deviation of 0.76. The responses showed limited variance, with 70 participants confirming it as one of the methods, 21 stating it was not, and 33 participants reporting insufficient information. The results also reveal similar variance in respondents' opinions on other aspects. Meetings with specialists for school students to raise cybersecurity awareness received a mean score of 1.94 and a standard deviation of 0.78. Similarly, using SMS messages for cybersecurity awareness had a mean score of 1.93 and a standard deviation of 0.79.

Additionally, the possibility of holding scientific conferences with media institutions regarding cybersecurity had a mean score of 1.81 and a standard deviation of 0.73. The homogeneity in mean values and the low variance suggest that respondents' answers across these methods were relatively similar. While some participants indicated the existence of these plans and methods in their institutions, others denied their presence, and some lacked definite knowledge on the subject. These findings align with the study by Al-Omairi et al. (2024), which highlighted the reliance on digital media strategies in Kuwait to promote cybersecurity awareness.

Hypotheses

There is a significant statistical relationship between the implementation of legislation and laws and the level of response to cybersecurity threats in national institutions

Table 9 presents the Spearman correlation coefficient between "legislation and laws related to cybersecurity" and "the level of response to cybersecurity threats." The correlation value between these variables was 0.246**, with a significance level of 0.006, which is less than 0.01. This indicates a weak direct relationship between the two.

The weak correlation suggests a limited practical impact of cybersecurity laws on national institutions' response to threats. This finding highlights systemic challenges, including insufficient enforcement mechanisms and a lack of awareness among communicators.

While the study identified a statistically weak correlation between legislation and response to cybersecurity threats (Spearman's rho = 0.246, $p = 0.006$), it is crucial to explore the potential reasons behind this finding. Several cultural, organizational, and contextual factors may be influencing these weak associations, highlighting broader challenges in cybersecurity implementation within national institutions.

One possible explanation lies in cultural attitudes toward compliance and cybersecurity awareness. In some Middle Eastern contexts, including Kuwait, cybersecurity is often viewed as a technical issue rather than an institutional priority (Hassib and Shires, 2022). This perception may result in legislation being seen as reactive rather than preventive, leading to low engagement from communicators who do not perceive direct accountability for cybersecurity measures. Additionally, research suggests that hierarchical organizational cultures in the region may discourage proactive cybersecurity behaviors, as employees often defer responsibility to IT departments rather than integrating cybersecurity practices into their daily communication strategies (Almutairi, 2023).

Another contributing factor could be institutional gaps between policy and enforcement. Although Kuwait has established cybersecurity legislation, including regulatory frameworks under CITRA, the practical implementation remains inconsistent (Mijwil et al., 2023). Studies indicate that many national institutions lack clear cybersecurity protocols, structured training programs, or enforcement mechanisms, leading to limited responsiveness even when legislation exists (Al-Mutairi and Al-Suhail, 2022). Moreover, cybersecurity measures often focus on technical infrastructure rather than human-centric approaches, meaning that communicators-who play a vital role in cybersecurity awareness-may not be sufficiently trained or empowered to implement these laws effectively. Another critical aspect influencing weak correlations could be the institutional prioritization of cybersecurity. Many public-sector institutions in Kuwait face competing administrative and budgetary priorities, which may result in cybersecurity policies receiving less attention compared to other national security concerns (Mallick and Nath, 2024). Additionally, legislation alone may not be sufficient to drive proactive cybersecurity engagement unless accompanied by strong institutional incentives, training programs, and stakeholder engagement strategies (Elareshi et al., 2024).

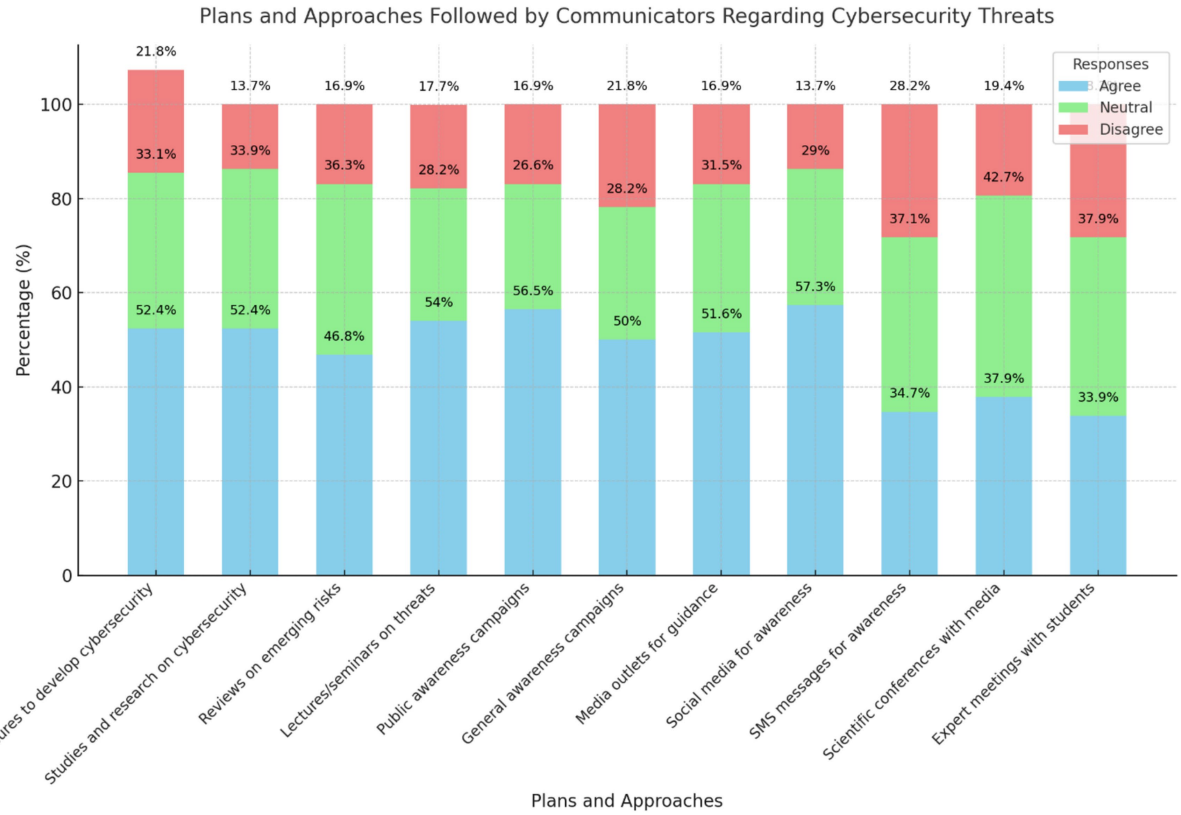

FIGURE 8
Plans and approaches followed by the communicator regarding cybersecurity threats.

Thus, these findings suggest that merely having cybersecurity legislation is not enough to ensure strong institutional responses. Future research should focus on examining organizational leadership's role in cybersecurity policy enforcement; investigating institutional cybersecurity training gaps and how they affect compliance; and exploring cross-national comparisons to identify best practices for aligning cybersecurity legislation with effective institutional response strategies. By addressing these factors, national institutions can move beyond a legislative approach and foster a cybersecurity culture that integrates awareness, engagement, and active threat response.

Hence, despite the weak relationships, these findings underscore the need for targeted policy interventions, including enhanced training programs for communicators and the development of operational frameworks to bridge the gap between legislation and practice. Furthermore, these results emphasize the importance of aligning policies with institutional capabilities to ensure effective implementation. Future studies should explore alternative methodologies or mixed-method approaches to capture the clear relation between laws and cybersecurity practices more comprehensively.

There is a significant statistical relationship between the existence of legislation and laws related to cybersecurity and the powers granted to those in charge of it in national institutions

Table 10 presents the Spearman correlation coefficient between the variable "powers granted to those in charge of cybersecurity" and the variable "existence of legislation and laws." The correlation value between these variables was 0.040, with a significance level of 0.655, which is higher than 0.01. This indicates an extremely weak positive relationship. Since the correlation is not statistically significant, it can be considered negligible. The weak correlation ($r = 0.040$, $p = 0.655$) suggests that existing laws may not sufficiently empower individuals responsible for cybersecurity. This finding points to ambiguities in legislative provisions and gaps in their practical implementation. These issues could limit the effectiveness of cybersecurity personnel. To improve their role in mitigating cyber threats, legislative reforms and clearer enforcement mechanisms are recommended.

There is a significant statistical relationship between curbing spam messages and responding to cyber incident threats by the communicator in national institutions

Table 11 presents the Spearman correlation coefficient between the variable "response to cybersecurity threats" and the variable "suppressing intrusive messages." The correlation value between these variables was 0.029, with a significance level of 0.748, which is higher than 0.01. This indicates an extremely weak positive relationship. Since the correlation is not statistically significant, it can be considered negligible.

The weak correlation ($r = 0.029$, $p = 0.748$) may be due to the limited scope of spam legislation in addressing broader cybersecurity challenges. Anti-spam measures often rely heavily on technical tools, with minimal involvement from communicators. This reduces their direct influence on incident response. Additionally, communicators

TABLE 8 Plans and approaches followed by the communicator regarding cybersecurity threats.

Plans and approaches followed by the communicator regarding cybersecurity threats		Frequencies	Percentage	Mean	Standard deviation	Range
There are measures to develop cybersecurity.	Agree	56	52.4%	1.76	0.78	2
	Neutral	41	33.1%			
	Disagree	27	21.8%			
There are studies and researches on cybersecurity	Agree	65	52.4%	1.61	0.71	2
	Neutral	42	33.9%			
	Disagree	17	13.7%			
There are reviews regarding cybersecurity and emerging or potential risks	Agree	58	46.8%	1.70	0.74	2
	Neutral	45	36.3%			
	Disagree	21	16.9%			
There are lectures and seminars on cybersecurity threats.	Agree	67	54%	1.63	0.76	2
	Neutral	35	28.2%			
	Disagree	22	17.7%			
There are lectures and public awareness campaigns on cybersecurity.	Agree	70	56.5%	1.60	0.76	2
	Neutral	33	26.6%			
	Disagree	21	16.9%			
There are awareness campaigns for the public about cybersecurity.	Agree	62	50%	1.71	0.80	2
	Neutral	35	28.2%			
	Disagree	27	21.8%			
Various media outlets are used for awareness and guidance regarding cybersecurity.	Agree	64	51.6%	1.65	0.75	2
	Neutral	39	31.5%			
	Disagree	21	16.9%			
Social media is used for cybersecurity awareness	Agree	71	57.3%	1.56	0.72	2
	Neutral	36	29%			
	Disagree	17	13.7%			
SMS messages are used for cybersecurity awareness.	Agree	43	34.7%	1.93	0.79	2
	Neutral	46	37.1%			
	Disagree	35	28.2%			
The possibility of holding scientific conferences with media institutions regarding cybersecurity.	Agree	47	37.9%	1.81	0.73	2
	Neutral	53	42.7%			
	Disagree	24	19.4%			
The presence of experts meetings with school students to raise their awareness on cybersecurity	Agree	42	33.9%	1.94	0.78	2
	Neutral	47	37.9%			
	Disagree	35	28.2%			

TABLE 9 Testing the validity of the first hypothesis.

Item		Legislation and laws related to cybersecurity		
		Unauthorized access to computers, systems and data	Unauthorized interference, interception, modification or destruction of computers, systems and data	Data protection and privacy
Level of response to cybersecurity threats	Correlation coefficient Spearman's rho	0.246**		
	Significance level. Sig. (2-tailed)	0.006		

may lack sufficient awareness or training regarding the impact of spam regulations on broader cybersecurity responses. To address this, enhanced training for communicators is needed (Muhammad and Adel, 2024). This training should focus on integrating spam control strategies into comprehensive cybersecurity practices.

There is a significant statistical relationship between the plans and methods used to address cybersecurity threats, and the presence of laws or procedural regulations for cybercrimes in national institutions

Table 12 presents the Spearman correlation coefficient between the variable "plans and methods for addressing cybersecurity threats" and the variable "presence of legislations and laws." The correlation value between these variables was −0.029, with a significance level of 0.737, which is higher than 0.01. This indicates an extremely weak negative relationship. Since the correlation is not statistically significant, it can be considered negligible.

The weak negative correlation ($r = -0.029$, $p = 0.737$) suggests potential inconsistencies between established plans and existing procedural laws. There are several possible reasons for this. Institutions may adopt cybersecurity plans independently, without aligning them with procedural laws. This can lead to fragmented strategies. Additionally, while cyber threats evolve rapidly, legislation often lags behind, making existing laws insufficient to guide new cybersecurity plans. To address this, regular updates to procedural laws are necessary. These updates should be informed by emerging threats and institutional practices to close the gap.

Overall, these findings lay the foundation for further analysis, particularly regarding institutional readiness and legislative effectiveness. The interpretation of the results provides broader implications for communicators' attitudes toward cybersecurity.

Given the findings and discussions presented, the next section concludes the research by highlighting its theoretical, practical, and policy implications, along with recommendations for future work in this area.

TABLE 10 Testing the validity of the second hypothesis.

Item		Authorities granted to those in charge of cybersecurity
Existence of legislations and laws	Correlation coefficient Spearman's rho	0.040
	Significance level. Sig. (2-tailed)	0.655

Conclusion

This study investigated the attitudes and preparedness of communicators in Kuwaiti national institutions toward cybersecurity, emphasizing the role of legislative frameworks, communication strategies, and their integration into national cybersecurity efforts. The findings highlight notable gaps in communicators' awareness and preparedness, as well as disparities in methods employed to address cybersecurity threats. While some institutions demonstrated active engagement through training programs, awareness campaigns, and collaborations, others lacked structured plans or sufficient knowledge of cybersecurity legislation. The research underscores the pivotal role of communicators in bridging technical expertise and public understanding of cybersecurity. By applying the TAM, the study revealed how perceived usefulness and ease of use influence communicators' adoption of cybersecurity practices. Aligning communication strategies with legislative frameworks emerged as a crucial factor for strengthening the nation's cybersecurity posture.

This study is directly relevant to the research topic as it examines how communicators' attitudes, institutional policies, and cybersecurity legislation interact to shape national security strategies. The findings highlight the importance of integrating communicators into cybersecurity decision-making processes, reinforcing the significance of communication strategies in mitigating cyber threats. The study provides actionable recommendations for policymakers and institutional leaders to enhance cybersecurity resilience through targeted awareness programs, legislative improvements, and cross-sector collaborations. By situating communicators at the center of cybersecurity strategies, this research underscores their critical role in strengthening national cybersecurity frameworks.

From a practical standpoint, this study emphasizes the need for enhancing cybersecurity readiness by addressing the human and communicative dimensions, moving beyond purely technical solutions. Actionable recommendations include mandatory training programs tailored for communicators, stronger legislative awareness initiatives, integration of communicators into cybersecurity teams, targeted public campaigns, and fostering cross-sector collaborations. Additionally, the study suggests leveraging technology for training, creating incentives for proactive participation, and establishing a national cybersecurity forum to encourage dialogue and innovation. The broader significance of these findings lies in their implications for academics, practitioners, and policymakers. For researchers, the integration of TAM provides a novel framework to explore human dimensions of cybersecurity communication. For practitioners, the

TABLE 11 Tests the validity of the third hypothesis.

Item		Response to cybersecurity threats		
		Presence of a team for responding to computer incidents	Presence of a team for responding to security incidents	Presence of a team for responding to computer emergencies
Curbing spam messages	Correlation coefficient Spearman's rho	0.029		
	Significance level. Sig. (2-tailed)	0.748		

TABLE 12 Tests the validity of the fourth hypothesis.

Item		Plans and methods to address cybersecurity threats
Existence of legislations and laws	Correlation coefficient Spearman's rho	−0.029
	Significance level. Sig. (2-tailed)	0.737

study highlights the critical role of communicators in ensuring institutional resilience. For policymakers, it offers actionable strategies for designing more inclusive and effective national cybersecurity frameworks (Al-Bawwab, 2014). By bridging gaps between policy, practice, and communication, this study lays the foundation for future research and initiatives aimed at enhancing cybersecurity preparedness in national institutions, fostering a culture of awareness, resilience, and collaboration. Thus, this study not only bridges a significant gap in the literature but also offers context-specific insights that can inform broader regional and global cybersecurity practices.

Limitations of the study

The following section acknowledges the limitations of this research. Such as, this study is geographically confined to Kuwait and institutionally limited to its national institutions. While this focused scope enables an in-depth understanding of local cybersecurity practices, it narrows the applicability of the findings to other regions or international contexts. Cybersecurity attitudes and challenges can vary significantly across nations due to differences in legislative frameworks, technological adoption, and institutional priorities (Mallick and Nath, 2024).

For instance, while Kuwaiti institutions prioritize cybersecurity to safeguard vital sectors like oil and public services, institutions in other regions may face different challenges, such as securing diverse, decentralized infrastructures. Comparative studies across multiple nations would provide broader insights into how geographic and institutional differences influence cybersecurity attitudes and practices. The study's findings should be viewed as a case study rather than universally applicable conclusions, providing a foundation for similar research in other geopolitical contexts. The confidentiality restrictions of some institutions posed challenges in data collection, potentially affecting the comprehensiveness of the findings. Such restrictions are common in studies involving sensitive topics like cybersecurity, as organizations often limit data sharing to protect operational security (Huzaizi et al., 2021). While these constraints are understandable, they highlight the need for alternative approaches to enhance data reliability, such as anonymized datasets, indirect surveys, or interviews with third-party experts. These methods can help mitigate the impact of restricted access while ensuring the richness of data collected. Future research should also aim to establish partnerships with organizations to access non-confidential, aggregate-level data, promoting a more transparent research environment.

Significance of the study

Here are the strengths and significance of the current research. This study makes valuable contributions on multiple levels. Theoretically, it enhances existing frameworks by integrating the Technology Acceptance Model (TAM) to explore communicators' attitudes toward cybersecurity, addressing a gap in the literature that often overlooks the human and communicative dimensions. Practically, the findings provide actionable insights for policymakers, organizational leaders, and cybersecurity trainers to design targeted training programs and awareness campaigns, empowering communicators to play a proactive role in cybersecurity strategy. From a policy perspective, the study identifies gaps in communicators' preparedness and supports the refinement of legislative frameworks, such as Kuwait's Communication and Information Technology Regulatory Authority initiatives, to align institutional practices with global standards. By focusing on communicators in Kuwaiti national institutions, this research offers context-specific insights that contribute to a broader understanding of cybersecurity within the Arab world, emphasizing the critical role of human factors in addressing cyber threats effectively.

Context specific actionable steps and implementation of cybersecurity recommendations in Kuwait

The following actionable steps outline how the study's recommendations can be effectively integrated within Kuwait's cybersecurity framework to enhance cybersecurity resilience within Kuwaiti national institutions. Firstly, role of Communicators should be enhanced in cybersecurity decision-making. For this, Kuwaiti national institutions should establish dedicated cybersecurity communication units within governmental agencies and media organizations (Al-Enezi et al., 2014). These units should work closely with CITRA (Communications and Information Technology Regulatory Authority) to ensure consistent messaging and policy dissemination. Moreover, developing inter-agency collaboration frameworks will help bridge the gap between cybersecurity experts, policymakers, and communicators, ensuring that cybersecurity policies are well understood and properly implemented across institutions. Such as, the Kuwaiti government could introduce an annual cybersecurity awareness summit where communicators and technical experts share insights, discuss emerging threats, and develop unified strategies for public cybersecurity education campaigns.

Secondly, national cybersecurity training initiatives should include specialized modules for communicators, focusing on; cyber threat recognition and reporting mechanisms, best practices in crisis communication during cybersecurity incidents, and handling misinformation and fake news related to cyber threats. Government institutions, in collaboration with Kuwaiti universities and cybersecurity think tanks, should integrate cybersecurity awareness courses into journalism and mass communication curricula (Corradini, 2020). For example, CITRA and the Ministry of Information could develop certification programs for communicators, ensuring that media professionals and institutional spokespersons are equipped with cybersecurity expertise.

Thirdly, the Kuwaiti government should launch nationwide awareness campaigns targeting both institutional employees and the

general public. These campaigns should be multilingual (Arabic and English) to ensure accessibility for expatriates working in national institutions. These campaigns should utilize popular Kuwaiti social media platforms like Twitter/X, Instagram, Snapchat, ensuring maximum reach and engagement. For instance, a public-private partnership between the government and media agencies could fund interactive workshops, televised debates, and digital infographics to educate employees and the public about cybersecurity risks and best practices. Fourthly, Kuwaiti national institutions should develop standard operating procedures (SOPs) that explicitly define the role of communicators in cybersecurity crisis management. Communicators should be included in cybersecurity emergency response teams (CERTs) to ensure accurate and timely dissemination of information during cyberattacks. Like, during a ransomware attack on a government database, pre-trained communicators could issue verified public statements to prevent misinformation, thereby maintaining public trust and institutional credibility.

Lastly, Cybersecurity laws in Kuwait should be updated regularly to reflect emerging threats such as AI-driven cyberattacks and deepfake misinformation campaigns. In addition, to ensure compliance, the government should introduce mandatory cybersecurity audits for institutions handling sensitive national data, with communicators playing a role in public reporting and accountability. For instance, the National Cybersecurity Authority (NCA) could publish annual reports on cybersecurity readiness, using communicators to translate technical reports into accessible public awareness content. Hence, by contextualizing these recommendations, Kuwaiti national institutions can ensure that cybersecurity strategies are both practical and culturally relevant. The integration of communicators into cybersecurity planning and incident response will enhance institutional preparedness, reduce public misinformation during crises, and strengthen national resilience against cyber threats.

Recommendations for future research

The following section contextualizes the findings for the future research recommendations. This study highlights communicators' roles in cybersecurity within Kuwaiti institutions but identifies areas for further exploration to enhance understanding and applicability. Future research should examine communicators in different regions, especially GCC states, and private-sector organizations like financial and tech firms, to assess cross-contextual findings. Employing qualitative or mixed-methods approaches, such as interviews or focus groups, could provide deeper insights into their experiences. Additionally, investigating emerging technologies like AI and blockchain, along with their ethical implications, could enhance cybersecurity communication strategies. Longitudinal studies tracking changes in communicators' roles over time would offer insights into evolving challenges and the effectiveness of training programs. Exploring cross-sector collaboration between government, academia, and private organizations, as well as public perceptions of communicators' credibility, could improve communication strategies. Demographic factors, such as age, gender, and education, should also be analyzed to address diverse challenges, while studies on leadership support and institutional policies can reveal how they shape effective communication frameworks. By addressing these areas, future research can enhance communicators' contributions to cybersecurity, inform training programs, and support policy development, ensuring that human dimensions remain central to national cybersecurity strategies.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. Written informed consent from the [patients/ participants OR patients/participants legal guardian/next of kin] was not required to participate in this study in accordance with the national legislation and the institutional requirements.

Author contributions

HM: Formal analysis, Investigation, Supervision, Visualization, Writing – original draft. MQ: Conceptualization, Project administration, Visualization, Writing – original draft.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. This work was supported and funded by Kuwait University, Research Grant No. AM01/24.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that no Gen AI was used in the creation of this manuscript.

Publisher's note

References

Al Doghmi, A., Al-Shalabi, H., Odeh, J. M., Andraws, S., Awajan, A., and Alrabea, A. I. (2013). The academic use of social networks among university students in Jordan. *Int. J. Comput. Sci. Issues* 10:134.

Al Hadeed, A. Y. B., Al-khatib, A. W., Al Olaimat, F., Habes, M., Alhammad, K. L., and Valeri, M. (2024). "Fostering organizational image: the direct roles of big data analytics, radical innovation, and incremental innovation capabilities" in Knowledge management and knowledge sharing: Business strategies and an emerging theoretical field (Switzerland: Springer), 75–85.

Al Olaimat, F., Habes, M., Hadeed, A., Yahya, A., and Al Jwaniat, M. I. (2022). Reputation management through social networking platforms for PR purposes: a SEM-based study in the Jordan. *Front. Commun.* 7:247. doi: 10.3389/fcomm.2022.1009359

Al-Amiri, M. (2024). Electronic media journalist in Kuwait towards cyber security. *Arab J. Human Sci.* 42, 11–42.

Albannai, N. A. A., Raziq, M. M., Malik, M., and Abrar, A. (2024). Digital leadership and its impact on agility, innovation and resilience: A qualitative study of the UAE media industry. UK: Benchmarking: An International Journal.

Al-Bawwab, Muhammad. (2014). The impact of the participatory learning method in an electronic environment on developing programming language skills among female first-year secondary school students in Al-Mikhwah governorate. UK.

Al-Enezi, K. A., Al-Shaikhli, I. F., Al-Kandari, A. R., and Aldabbagh, S. S. M. (2014). "Cyber-attacks Detection & Protection in Kuwait government sectors" in In 2014 3rd international conference on advanced computer science applications and technologies (UK: IEEE), 50–55.

Al-Hamad, K. L. (2023). The Jordanian public's reliance on public relations campaigns as a source of information during the COVID-19 pandemic (Jordanian TV and Kingdom Channels).

Alhanatleh, H., Alghizzawi, M., Habes, M., Tahat, K., and Tahat, D. N. (2023). The impact of digital marketing through the Tik Tok application on purchase intent. 2023 tenth international conference on social networks analysis, management and security (SNAMS), 1–6.

Al-Janafawi, K. M. (2023). The Level of Security & the Requirements of Sustainable Security in the Kuwaiti society according to the Viewpoint of the Employees of the Saad Al-Abdullah Academy for Security Sciences and its Relationship to some Variables. *Annals of the Faculty of Arts, Ain Shams University.* 51, 338–376.

Al-Jenfawi, K. M. (2023). The role of the family in confronting the excessive use of modern technology among children" therapeutic alternatives". *J. Police Legal Sci.* 14:5. doi: 10.69672/3007-3529.1020

Almutairi, K. (2023). Cybersecurity awareness in the Middle East: challenges and opportunities. *J. Cybersecur. Stud.* 8, 101–119. doi: 10.1016/j.jcss.2023.08.005

Al-Mutairi, K., and Al-Suhail, J. (2022). The role of criminal regulations in protecting cybersecurity in the Gulf cooperation council countries. *J. Legal Jurisprudence* 34, 969–1066.

Alnujaifi, M., Atallah, M. N., Alheety, N. A., Al Enizi, Z., and Madi, R. (2024). Regulatory framework governing the right to information in the United Arab Emirates: an analytical examination. *Global Privacy Law Rev.* 5, 99–108. doi: 10.54648/GPLR2024015

Al-Omairi, M., Alamir, S. G., Salman, B. I., El Deeb, S., Alrashdi, Y. B. A., Al-Harrasi, A., et al. (2024). Investigating trace and macro-element composition of herbal and nutraceutical dietary supplements marketed in Oman: insights into safety and Labeling. *Biol. Trace Elem. Res.* 203, 2911–2923. doi: 10.1007/s12011-024-04343-w

Al-Otaibi, A. Sh. (2020). The role of cybersecurity in achieving vision 2030 (unpublished master thesis). Nayef Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia. Available at: https://journals.nauss.edu.sa/index.php/JISCR/article/view/1225.

Al-Shammari, M I S. (2021). Cybersecurity and its impact on Iraqi national security. UK.

Attar, R. W., Habes, M., Almusharraf, A., Alhazmi, A. H., and Attar, R. W. (2024). Exploring the impact of smart cities on improving the quality of life for people with disabilities in Saudi Arabia. *Front. Built Environ.* 10:1398425. doi: 10.3389/fbuil.2024.1398425

Ben Jeddou, B. (2022). Cybersecurity challenges in confronting cybercrime. *Algerian J. Human Secur.* 7, 299–319.

Ben Romdhane, S., Elareshi, M., Habes, M., Alhazmi, A. H., and Attar, R. W. (2025). Connecting with the hyper (dis) connected audience: university communication attributes and student attitudes. *SAGE Open* 15:21582440251341056. doi: 10.1177/21582440251341058

Bornstein, M. H., Jager, J., and Putnick, D. L. (2013). Sampling in developmental science: situations, shortcomings, solutions, and standards. *Dev. Rev.* 33, 357–370. doi: 10.1016/j.dr.2013.08.003

Cambria, E., Kumar, A., Al-Ayyoub, M., and Howard, N. (2022). Guest Editorial: Explainable artificial intelligence for sentiment analysis. *Knowl. Based Syst.*, 238, 107920.

Corradini, I. (2020). Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology, UK. 284.

Cyber Security Agency of Singapore. (2023). Cybersecurity strategy in Singapore: national priorities and implementation roadmap. Available online at: https://www.csa.gov.sg (Accessed February 22, 2024).

Cybersecurity and Infrastructure Security Agency. (2022). CISA'S role in national cybersecurity coordination. Available online at: https://www.cisa.gov

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* 13, 319–340. doi: 10.2307/249008

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Bus. Inf. Rev.* 35, 60–67. doi: 10.1177/0266382118773624

Dawson, G., Rogers, S., Munson, J., Smith, M., Winter, J., Greenson, J., et al. (2023). Randomized, controlled trial of an intervention for toddlers with autism: the early start Denver model. *Pediatrics* 125, e17–e23.

Department of Homeland Security. (2023). Cyber storm VIII: national cybersecurity resilience exercise. Available online at: https://www.dhs.gov/cyber-storm (Accessed December 1, 2024).

Dumpit, D. Z., and Fernandez, C. J. (2017). Analysis of the use of social media in higher education institutions (HEIs) using the technology acceptance model. *Int. J. Educ. Technol. High. Educ.* 14:5. doi: 10.1186/s41239-017-0045-2

e-Governance Academy. (2023). Cybersecurity education in Estonia: Integrating digital governance into national curricula. Available online at: https://www.ega.ee (Accessed July 10, 2024).

Elareshi, M., Habes, M., Ahmad, N., Ali, S., and Attar, R. W. (2024). Public engagement through public service advertisements for health care awareness during early COVID-19 in Pakistan. *Front. Commun.* 9:1376717.

Enaya, A. H., and Enaya, H. A. (2014). Scientific research, including collection, investigation, and study. *J. Islamic Girls College Assyout* 16, 805–901.

Etikan, I., Musa, S. A., and Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *Am. J. Theor. Appl. Stat.* 5, 1–4. doi: 10.11648/j.ajtas.20160501.11

European Commission. (2023). General data protection regulation (GDPR) and cybersecurity enforcement. Available online at: https://ec.europa.eu (Accessed September 11, 2024).

Eyadat, W. M. (2024) Social media users and cybersecurity awareness: an international perspective. Egypt - Cairo.

Gao, C. A., Howard, F. M., Markov, N. S., Dyer, E. C., Ramesh, S., Luo, Y., et al. (2023). Comparing scientific abstracts generated by ChatGPT to real abstracts with detectors and blinded human reviewers. *NPJ Digital Medicine* 6:75. doi: 10.1038/s41746-023-00819-6

Habes, M., Alghizzawi, M., Youssef, E., and Al-Zoubi, A. F. (2024). The impact of media technology on family relations during crisis. *Opportunit Risks AI Business Develop.* 1:27.

Habes, M., Ali, S., and Pasha, S. A. (2021). Statistical package for social sciences acceptance in quantitative research: from the technology acceptance model's perspective. *FWU J. Soc. Sci.* 15, 34–46. doi: 10.51709/19951272/Winter-2021/3Statistical

Habes, M., Elareshi, M., Mansoori, A., Pasha, S., Salloum, S. A., and Al-rahmi, W. M. (2023). Factors indicating media dependency and online misinformation sharing in Jordan. *Sustain. For.* 15, 1–15. doi: 10.3390/su15021474

Haleem Shaikh, S., Shaikh, H., and Shaikh, S. (2019). The impact of extrinsic motivation on employees' performance: a case study of food Industries in Sindh, Pakistan. Technology, and sciences (ASRJETS) American scientific research journal for. *Engineering* 56, 26–37.

Hamzah, N., Mohd Saman, H., Baghban, M. H., Mohd Sam, A. R., Faridmehr, I., Muhd Sidek, M. N., et al. (2022). A review on the use of self-curing agents and its mechanism in high-performance cementitious materials. *Buildings* 12:152. doi: 10.3390/buildings12020152

Han, M., and Zhang, X. (2020). Prospects for the advancement of the Tik Tok in the age of 5G communication. 2020 13th CMI conference on cybersecurity and privacy (CMI)-digital transformation-potentials and challenges (51275), 1–5.

Hassib, B., and Shires, J. (2022). Cybersecurity in the GCC: from economic development to geopolitical controversy. *Middle East Policy* 29, 90–103. doi: 10.1111/mepo.12616

Huzaizi, A. H. A., Tajuddin, S. N. A. A., Bahari, K. A., Manan, K. A., and Abd Mubin, N. N. (2021). Cyber-security culture towards digital marketing communications among small and medium-sized (SME) entrepreneurs. *Asian Cult. History* 13, 1–20.

Jager, J., Putnick, D. L., and Bornstein, M. H. (2017). More than just convenient: the scientific merits of homogeneous convenience samples. *Monogr. Soc. Res. Child Dev.* 82, 13–30. doi: 10.1111/mono.12296

Jamal Al-Din, H. (2023). Cybersecurity and transformation in the international system. *J. Facult. Econo. Polit. Sci.* 24, 189–230.

Khader, M., Karam, M., and Fares, H. (2021). Cybersecurity awareness framework for academia. *Information* 12:417. doi: 10.3390/info12100417

Khan, A., and Ahmed, A. (2024). Optimizing Retail Operations, Inventory Management and Sales Forecasting with Big Data and AI in China. *Emerging Trends in Machine Intelligence and Big Data*, 16, 18–37.

Lederer, A. L., Maupin, D. J., Sena, M. P., and Zhuang, Y. (2000). The technology acceptance model and the world wide web. *Decis. Support. Syst.* 29, 269–282. doi: 10.1016/S0167-9236(00)00076-2

Lee, S.-H., Kang, I., and Kim, H.-W. (2023). Understanding cybercrime from a criminal's perspective: why and how suspects commit cybercrimes? *Technol. Soc.* 75:102361. doi: 10.1016/j.techsoc.2023.102361

Mallick, M. A. I., and Nath, R. (2024). Navigating the cyber security landscape: a comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Sci. News* 190, 1–69.

Mansoori, A., Tahat, K., Tahat, D. N., Habes, M., and Salloum, S. A. (2024). "Optimizing news categorization with machine learning: a comprehensive study using naive Bayes (MultinomialNB) classifier" in Achieving sustainable business through AI, technology education and computer science: Volume 1: Computer science, business sustainability, and competitive advantage (Sweden: Springer), 169–178.

Mijwil, M., Aljanabi, M., and Ali, A. H. (2023). Chatgpt: exploring the role of cybersecurity in the protection of medical information. *Mesopotamian J. Cybersecur.* 2023, 18–21. doi: 10.58496/MJCS/2023/004

Muhammad, A.-S., and Adel, A. (2024). Constitutional protection of cybersecurity and its role in protecting the right to information privacy. *Spirit Laws* 36, 491–676.

Murad, K. (2023). The cognitive and skill-based implications of the digital environment on media education curricula in Jordanian universities - a field study. *An-Najah University J. Res. B: Humanities*. 37, 2187–2216.

Musallam, N. (2021). Cybercrimes and their impact on cyber security. *Al-Qadisiyah J. Law and Polit. Sci.* 12, 373–403.

Muslim, (2021). Netflix speaks Arabic, Arabs speak Netflix: How SVOD is transforming Arabic series screenwriting. *J. Arab Muslim Media Res*, 14, 261–280. doi: 10.1386/jammr_00034_1

National Cyber Security Centre. (2023). Building a unified national cybersecurity framework in the UK. Available at: https://www.ncsc.gov.uk (Accessed August 10, 2024).

National Institute of Information and Communications Technology. (2022). Cybersecurity education and workforce development in Japan. Available onine at: https://www.nict.go.jp (Accessed August 10, 2024).

Pawar, S., and Palivela, H. (2022). LCCI: a framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *Int. J. Inform. Manag. Data Insights* 2:100080. doi: 10.1016/j.jjimei.2022.100080

Sarwar, B., Sarwar, A., Mugahed Al-Rahmi, W., Almogren, A. S., Salloum, S., and Habes, M. (2023). Social media paradox: utilizing social media technology for creating better value for better social outcomes: case of developing countries. *Cogent Business Manag.* 10:2210888. doi: 10.1080/23311975.2023.2210888

Sen, A. (1994). Freedoms and needs. New republic, 210, 31–37.

Sharma, C., and Maurya, S. (2020). A review: importance of cyber security and its challenges to various domains. *Int. J. Technical Res. Sci.* 12, 46–54. doi: 10.30780/specialissue-icaccg2020/015

Shawirb, J., and Murad, F. (2023). The concept of cyber warfare and cyber security. *Law J.* 9.

Štitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., and Khorunzhak, N. (2020). Nationals cyber security strategies: management, unification and assessment. *Independent J. Manag. Product.* 11, 2341–2354. doi: 10.14807/ijmp.v11i9.1431

Tabassum, L., and Baker, S. (2020). Cybersecurity and safety measures. *Int. Res. J. Modern. Engin. Technol. Sci.* 2, 1357–1360.

Tahat, Z. Y., and Al-Mutairi, S. S. (2022). Dependency of Kuwaiti voters on social networking sites as a source of information about the 2016 parliamentary elections. *Egyptian J. Public Opinion Res.* 21, 457–503.

Tahat, K., Habes, M., Mansoori, A., Naqbi, N., Al Ketbi, N., Maysari, I., et al. (2024). Social media algorithms in countering cyber extremism: a systematic review. *J. Infrastruct. Policy Develop.* 8:6632. doi: 10.24294/jipd.v8i8.6632

Tahat, K., Mansoori, A., Tahat, D. N., Habes, M., and Salloum, S. (2023a). Leveraging soft power: a study of Emirati online journalism through Arabic topic Modeling. *Int. Conf. Business Technol.* 4, 13–20.

Tahat, K., Salloum, S., Mansoori, A., Tahat, D., Habes, M., Shaalan, K., et al. (2023b). "Uncovering the share fake news on social media during crisis" in 2023 tenth international conference on social networks analysis, management and security (SNAMS). 1–6.

Taherdoost, H. (2018). Sampling methods in research methodology; How to Choose a Sampling Technique for Research. Yarmouk.

Tarhini, A., Elyas, T., Akour, M. A., and Al-Salti, Z. (2016). Technology, demographic characteristics and E-learning acceptance: a conceptual model based on extended technology acceptance model. *High. Educ. Stud.* 6, 72–89. doi: 10.5539/hes.v6n3p72

Trigeassou, J. C., Maamri, N., Sabatier, J., and Oustaloup, A. (2011). A Lyapunov approach to the stability of fractional differential equations. *Signal Processing.* 91, 437–445.

Venkatesh, V., Davis, F. D., Hossain, M. A., Dwivedi, Y. K., Piercy, N. C., Hu, P. J., et al. (2000). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Manag. Sci.* 46, 319–340.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.