International Journal of Religion
2024
Volume: 5| Number 11 | pp. 932 – 946
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/frfnr583

Information Security for An Information Society for Accessing Secured Information: A PRISMA Based Systematic Review

Mohammad Rakibul Islam Bhuiyan[1], Md Wali Ullah[2], Shainjida Ahmed[3], Md Khokan Bhuyan[4], Tanzina Sultana[5] and Al- Amin[6]

Abstract

This study employs the PRISMA methodology to conduct a comprehensive review, aiming to examine the current state of information security in an information society. The study specifically focuses on the methods used to access protected information. The review consolidates findings from multiple scholarly sources, emphasizing common dangers, measures for mitigation, and optimal approaches to protecting digital information. The evaluation procedure involved conducting an extensive search across various academic databases such as Science Direct, Scopus, Web of Sciences, PubMed, and DOAJ, where a total of 105 documents were found, comprising 85 papers and 20 reports. The findings highlight the complex and diverse aspects of information security, emphasizing the need for a comprehensive approach that incorporates technological, organizational, and human components. The analysis demonstrates that although there have been notable advancements in the creation of advanced security measures, there are still obstacles to overcome, such as the emergence of new threats and the necessity for ongoing adjustment. The paper also highlights deficiencies in existing research, proposing areas for future exploration to strengthen the security position of information systems in a progressively networked world. This systematic review enhances existing knowledge by presenting a comprehensive overview of the current state of information security. It provides valuable insights for researchers, practitioners, and policymakers who are committed to safeguarding sensitive information in a society driven by information.

Keywords: *Information Securit, Secured Information, Information Society, PRISMA, Systematic Review*

INTRODUCTION

According to Hasnayen (2016), information is considered the lifeblood of contemporary organisations, serving as a crucial asset in the context of today's IT-enabled world. This is particularly evident in the case of governments, where the importance of information is paramount. The interconnectedness of IT systems and networks facilitates the exchange of data and provision of services among various organisations and individuals. The potential for both opportunities and challenges arises when considering the vulnerability of data if it is accessed by unauthorised sources (Thakuriah et al., 2017). According to Ismagilova et al. (2019), in order to ensure that citizens have access to and can benefit from high-quality information and services, it is crucial to design and construct information systems that are capable of efficiently collecting, analysing, and delivering the required information and services. Additionally, these information systems should be able to protect the confidentiality, integrity, and availability of the information and services they provide. There has been a

[1] Department of Management Information Systems, Begum Rokeya University, Rangpur, Rangpur-5404, Rangpur, Bangladesh. E-mail: rakib@mis.brur.ac.bd, ORCID: https://orcid.org/0000-0003-4284-6461

[2] MBA, Information Technology, Westcliff University, Irvine, United States of America. E-mail: M.Ullah.117@westcliff.edu, ORCID: https://orcid.org/0009-0009-5500-7377

[3] MBA and BBA major in Human Resource Management, Faculty of Business and Economics, Daffodil International University (DIU), Dhaka, Bangladesh. E-mail: s.a.prottasha@gmail.com, ORCID: https://orcid.org/0009-0008-2106-6187

[4] Master's of science in engineering Management, Westcliff University, 432 S New Hampshire Ave, United States of America. E-mail: m.bhuyan.573@westcliff.edu

[5] Information Technology, School of Business, Emporia State University,1 Kellogg Circle, Emporia, KS 66801, United States of America. E-mail: tsultana@g.emporia.edu ORCID ID: https://orcid.org/0009-0009-61681632

[6] MBA and BBA major in Marketing, Faculty of Business Studies, University of Dhaka. Dhaka-1000, Dhaka, Bangladesh. E-mail: alamin22.acc@gmail.com ORCID: https://orcid.org/0009-0001-1464-9631

significant amount of research conducted on the topic of information security, with a particular focus on cybercrime and ethical behaviour in relation to information.

Numerous studies have explored various aspects of these subjects, aiming to gain a deeper understanding of the challenges and implications they present. Researchers have examined different types of cybercrimes, such as hacking, identity theft, and online fraud, in order to identify patterns, motives, and potential countermeasures. Additionally, investigations have been carried out to investigate the ethical considerations surrounding the use and protection of information, including issues related to privacy, data breaches, and responsible information handling. These research efforts have contributed to the development of strategies and best practices for enhancing information security and promoting ethical behaviour in the digital age. In an attempt to ascertain the state of information security within the context of the information society, the researcher explored the perspectives of Bangladesh (Karlsson & Åstrom, 2015).

Information security refers to the safeguarding of all information assets from any type of misuse, damage, or unexpected consequences. This encompasses the protection of data stored in computer systems, ensuring the reliability of business operations, and keeping highly qualified employees along with their valuable expertise. Information and Communication Technology enables us to effectively utilise, access, and utilise information, as well as share knowledge in many human activities, leading to the development of economies and societies that are centred around information and knowledge. These platforms have the ability to facilitate the utilisation of diverse information by users, enabling them to make informed decisions and enhance the level of information security (Hadad, 2017).

The Internet, as a modern communication medium, has profoundly altered the manner in which individuals consume, work, and connect. Consequently, it has transformed society into what is widely recognised as the "Information Society" (Carmody, 2013). The phrase remains undefined and its consequences are not fully understood. Furthermore, Information security (InfoSec) also empowers organisations to safeguard both digital and analogue information. InfoSec encompasses the protection of encryption, mobile computing, social media, and infrastructure and networks that include private, financial, and business information (Weiss, 2010). Both government and private organisations employ information security for many reasons in the information society (Gil-Garcia & Pardo, 2005). The primary goals of InfoSec are often focused on guaranteeing the confidentiality, integrity, and availability of corporate information. InfoSec encompasses multiple domains and necessitates the deployment of diverse security measures, such as application security, infrastructure security, encryption, incident response, vulnerability management, and disaster recovery (Von Solms, & Van Niekerk, 2013).

Information system and network security have emerged as a fundamental concern in today's society due to the increasing significance of information in safeguarding and advancing human life on a daily basis. Litvinenko et al. (2022) asserted that industrialised countries have recognised the crucial importance of security and have implemented measures to tackle this issue. In contrast, developing countries are still far from being able to ensure this fundamental right. Risks to the Information Society were arising at various levels, including the content, network, and physical levels. However, technology alone cannot achieve information security. To effectively address network threats and establish a safe information society, it is imperative to implement both comprehensive preventive measures and enforcement measures (Bhuiyan et al., 2024).

Background Information

The government has demonstrated its dedication to ICT by sending a highly influential delegation led by the Honourable Prime Minister to the World Summit on the Information Society (WSIS). This delegation shares the collective vision of creating an information society that utilises the full potential of ICT to advance the development objectives outlined in the Millennium Declaration. These objectives include eliminating extreme poverty and hunger, ensuring universal primary education, and fostering global partnerships to achieve a more peaceful, equitable, and prosperous world (Al-Mamun et al., 2024). The Bangladesh Government, like other nations, acknowledges the crucial significance of science in the advancement of the information society (Bhuiyan et al., 2023). They also recognise the essential importance of education, knowledge, information, and communication in human development, progress, and well-being. The government has affirmed its

commitment to enable the impoverished, especially those residing in distant, rural, and marginalised urban regions, to obtain information and utilise ICTs as a means to aid their endeavours in escaping poverty.

Statement of the Problem

There is a significant amount of literature on the impact of ICT in different areas of society and socioeconomic progress, including education, administration, organizational dynamics, project management, service delivery, and healthcare (Poli et al., 2024). Information security in Bangladesh is a significant issue that can protect individuals, specific target groups, organizations, and even the state itself. In Bangladesh, the absence of information security prompts individuals to seek opportunities to exploit networks, systems, data, and operators for financial benefits (Islam & Bhuiyan, 2022). The researcher dedicates time and effort to facilitating access to information for all members of the information society. Furthermore, the significant impact of ICT on socioeconomic development is highlighted, demonstrating the interconnections between society, technology, business, and governmental policy (Islam et al., 2024).

Research Gap

Many underdeveloped nations, like Bangladesh, face constraints in accessing information. The available access is also not economical due to the insufficient infrastructure and lack of proper knowledge (Akhter et al., 2023). The issues arise from the absence of a cohesive computer security system and insufficient awareness regarding computer security (Yaacoub et al., 2022). Hence, it is imperative to foster cooperation, collaboration, and investment in order to enhance security measures and cultivate a culture that prioritises security concerns. In business and other interactions, trust is crucial and can be established when the participants have confidence in the security of the transaction (Bhuiyan et al., 2024). From a commercial standpoint, security should be regarded as a means to facilitate corporate operations rather than as an expense. Furthermore, it is imperative to implement additional initiatives focused on cybercrime legislation, as well as enhancing enforcement capacity building and conducting training courses across the entire nation (Eboibi, 2020). The country's policies should encompass privacy rules, trust marks, and other self-regulatory measures to facilitate the development of products and provision of services. Additionally, it is crucial to execute the required measures to establish customer confidence (Prastyanti, & Sharma, 2024).

Objectives of the Study

Identify alternative methods for securely obtaining information inside the information society.

Assess the information system security needs and priorities for a developing country such as Bangladesh.

Identify certain suggestions for securely sharing information with the information society.

LITERATURE REVIEW

Mishra and Dhillon (2010) defined information systems in the context of security governance as a means of creating and sustaining a controlled environment. This environment is necessary for the management of risks associated with the confidentiality, integrity, and availability of information and the processes and systems that support it. The current mechanical definition fails to consider the significance of the audit process for systems and the management of security details at the operational level of business processes. The Certified Information Systems Auditor (CISA) review manual defines information security governance as a focused activity that prioritises the integrity of information, continuity of services, and protection of information assets (Njenga & Brown, 2012).

Information security is a subject of increasing concern for the majority of enterprises. Based on the Global Security Survey conducted by Vielberth et al. (2020), the primary focus of concern in information security has shifted towards the human factor. The poll revealed that 91% of respondents expressed apprehension regarding staff security vulnerabilities, while 79% attributed information security failures to the human component. The insider threat poses a greater danger compared to external threats, as an individual with insider access can

quickly exploit their acquired skills and knowledge from lawful work responsibilities for unauthorised purposes (Willison & Siponen, 2009).

The implementation of appropriate security policies is essential for ensuring the successful governance of information system security. Creating a security policy that is easy to understand and provides all necessary information is crucial for effectively managing security. Disseminating these policies to employees improves their acceptance and leads to more effective application of those policies (Flores & Ekstedt, 2014). Researchers that prioritise the organisational aspect of comprehensive information system security governance contend that responsibility and accountability within organisational structures are crucial prerequisites for achieving successful security governance (Bhuiyan & Akter, 2024). Management establishes responsibility and accountability within organisational structures to cultivate a sense of ownership among employees towards information security procedures (Lee & Park, 2019).

Strict adherence to security governance rules can only be accomplished by implementing and enforcing internal controls. Regular evaluation of internal controls is crucial for optimising operational efficiency, resulting in reduced vulnerabilities and better-quality security management. Consequently, it is advisable to possess and implement systems and security procedures to achieve the desired outcome in security management (Rendon & Rendon, 2022).

The Information and Communication Technology Act and the Right to Information Act are significant laws pertaining to e-government (Ahmad, 2021). Bangladesh has been actively working towards implementing the e-Government Service Act and Digital Security Act, recognising the need for legal frameworks for cyber security and e-government. However, the proposed laws are either rejected or awaiting a decision.

Major ICT based Bangladeshi laws.

Table 1: Bangladesh's laws in ICT and e-Government

Category		Law
Foundation for Information Society		• Information & Communication Technology Act, 2009
Information Service Promotion	e-Government (Administration)	• Right to Information Act, 2009
	Promotion for informatization environment	• Bangladesh High-tech Park Authority Act • BCC Act, 1990
Adverse Effect Protection		• Information & Communication Technology Act, 2009 • Telecommunication Act, 2001 • Digital Security Act, 2018
ICT Industry Development		• Information & Communication Technology Act, 2009 • Telecommunication Act, 2001

Researchers stress the significance of including human factors in security management. They suggest that the governance of information systems security should align with management's aims, attitudes, and beliefs toward the organization's informational assets. Policies and controls lack human concerns (Bhuiyan et al., 2024). Effective execution of the rules and policies can only be achieved when individuals are capable of harmonizing their personal value system with the management. The researchers unanimously agree that when there is a mismatch between individual and corporate objectives, there is an increased risk of security breaches in

information systems by insiders within the organization. Therefore, it is recommended to regard employees as owners of information assets (Abdulrasool & Turnbull, 2020).

METHODOLOGY

The search was conducted utilizing widely recognized global databases including Science Direct, Scopus, Web of Sciences, PubMed, and DOAJ, in accordance with the guidelines outlined in the PRISMA statement of 2020 (Bhuiyan & Akter, 2024). The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) is a well-established and widely recognized framework that provides a standardized set of essential elements for accurately documenting and reporting the findings of meta-analyses and systematic reviews. It is based on rigorous evidence and has been extensively utilized in the field (Molla et al., 2023). The PRISMA guidelines primarily focus on promoting the accurate reporting of systematic reviews and meta-analyses that evaluate randomized controlled trials (RCTs). This framework can also be utilized as a structural basis for documenting systematic reviews of various types of research, particularly assessments of therapeutic interventions. Providing a comprehensive and detailed description of the techniques and results of systematic reviews is of utmost importance in order to enable consumers to assess the dependability and pertinence of the conclusions drawn from the review (Poli et al., 2024).

The research approach employed a systematic use of specific keywords, including but not limited to Information Systems, ICT laws, Information Society, Information Security, and priorities. Exclusion criteria are applied to eliminate any records that do not align with the selected keywords or study subjects, as stated by Molla et al. (2023). When making decisions about the rejection of publications and reports, it is important to take into account various additional factors (Mia et al., 2024). These factors include the availability of insufficient data, the presence of papers written in multiple languages, the existence of varied outcomes, and the disconnected nature of impacts and findings. During the examination, an additional 85 papers and 20 reports were discovered by the researchers, as depicted in Figure 1.

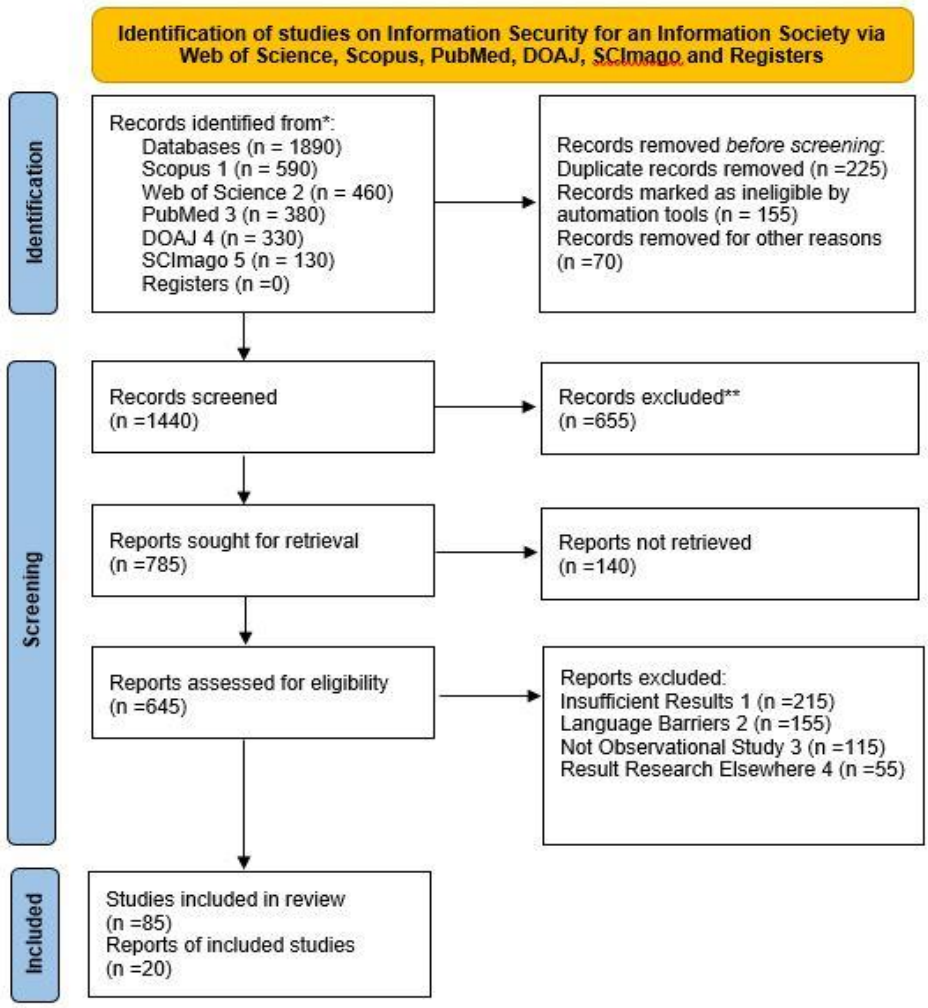

Figure 1: PRISMA Based Systematic Review

Source: (Haddaway et al., 2022).

DISCUSSION

Info-Tech determines its annual security objectives by gathering primary data through interviews with security and IT leaders. They also consider information from their 2023 Tech Trends research and the upcoming State of Hybrid Work in IT: A Trend research, which will be published in March 2023 in figure 2. The new security priorities report centres on data that provides specific information regarding the anticipated alterations in procedures and IT infrastructure as a result of hybrid work (Venkateswaran et al., 2022), apprehensions and perspectives concerning preparedness to comply with existing and forthcoming legislation, and the influence of a prospective economic downturn on security budgets in figure 2.

Figure 2: Security Priorities

Source: Info-Tech's Security Priorities 2023

During the pandemic, there has been a notable shift in the way individuals approach work, both in terms of their work practices and their preferred work locations. Many individuals have embraced a hybrid work model, which combines elements of remote work and in-person work. This model allows individuals to have more flexibility in choosing when and where they work, while still maintaining some level of face-to-face interaction (Venkateswaran et al., 2022). It is worth noting that this preference for a hybrid work model has persisted even as the pandemic situation has evolved. Notwithstanding the multitude of cybersecurity risks, organizations persist in their pursuit of modernization plans, driven by the overarching advantages they offer in the long run (Burns et al., 2019). The frequency of government-enacted regulatory changes is steadily rising. Instead of perceiving these changes as a mere compliance burden, it is advisable for organizations to view them as a valuable opportunity to enhance their security practices. The ongoing dynamic between threat actors and defenders resembles a cat-and-mouse game. The inquiry regarding the potential for improvement among defenders has been addressed through the expeditious advancement of technology. Typically, software development occurs within the context of a supply chain rather than in isolated environments. This means that software is often created as a collaborative effort involving multiple stakeholders and interconnected processes. As evidenced by recent occurrences, such as the Log4j and Solar Winds incidents, it has become apparent that the presence of a vulnerability within any component of the supply chain has the potential to serve as a vector for threats.

Information Security in Worldwide Perspective

The diverse manifestations of information are the paramount resource of an organization. Consequently, lapses in information security not only jeopardize the credibility of companies but also pose a potential threat to their survival (Burns et al., 2019). Global Perspective seeks to encompass a wide array of topics and ideas that are relevant to the field of information security. Our goal is to offer a comprehensive understanding of contemporary concerns in the field of professional information security (Anu, 2022). This will be achieved through an in-depth exploration of research and development, emerging technologies, tools, and practices, as well as anticipated future challenges. The United States will employ all available means of national influence to disrupt and dismantle individuals or groups whose actions pose a threat to our interests (L. Y. Hunter et al.,

2024). These endeavors may incorporate diplomatic, informational, military (including both physical and cyber aspects), financial, intelligence, and law enforcement capabilities in figure 3.

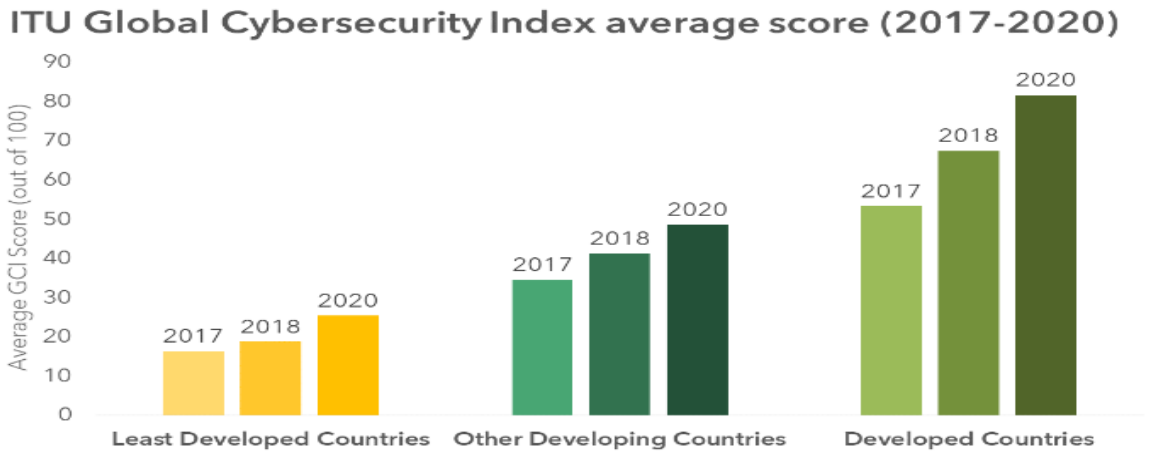

Figure 3: Cyber Security Average Score (World-wide)

Source: ITU Global Cybersecurity Index 2020

How To Develop a Global Perspective in Information Security?

Information security is a rapidly changing and intricate domain that necessitates ongoing education and adjustment. Nevertheless, if you solely concentrate on your immediate surroundings and difficulties, you can overlook useful perspectives and prospects from different areas and societies (Taskeen & Garai, 2024). Acquiring a comprehensive understanding of information security on a global scale can assist in improving your abilities, expanding your professional connections, and enhancing the equilibrium between your work and personal life. Here are some guidelines on how to accomplish the task.

Table 2: Global Perspective of IS

Global Perspective of IS	Description	Reference
Learn from diverse sources	A simple method to broaden one's worldview is to absorb information from many sources and perspectives. One can stay updated on information security by subscribing to the blogs, podcasts, newsletters, and social media accounts of global information security specialists and organizations. Additionally, you have the option to peruse books, articles, reports, and case studies that delve into various facets and concerns of information security within diverse contexts. By acquiring knowledge from a variety of sources, you can develop a more profound comprehension of the worldwide patterns, difficulties, and possibilities in the field of information security.	(Chen, 2017) (Riahi & Islam, 2024) (Ware & Healey, 2018)
Engage with global communities	One further method to cultivate a worldwide outlook is to actively participate in information security communities that transcend national and cultural boundaries. One can participate in online forums, groups, chats, and platforms to engage with information security professionals and enthusiasts from many countries and backgrounds. Additionally, you have the opportunity to engage in webinars, workshops, conferences, and events that facilitate connections with the worldwide information security community. By actively participating in international communities, you have the opportunity to share and receive ideas, experiences, feedback, and support from your colleagues and mentors.	(Aksoy, 2024) (Olson et al., 2024)
Work on cross-cultural projects	An effective method to cultivate a comprehensive understanding of global affairs is to engage in information security initiatives that require cooperation and communication across different cultures. Seek out possibilities to participate in or take charge of teams focused on global-scale information security initiatives. Additionally, you have the option to engage in volunteer work or make contributions to information security initiatives that provide assistance to social causes or communities throughout various regions of the globe. Engaging in cross-cultural initiatives enables the development of technical, interpersonal, and leadership proficiencies.	(Riahi & Islam, 2024) (Sylwia et al., 2024)
Travel and explore	One can cultivate a broader worldview by embarking on journeys to diverse locations and immersing oneself in various cultures. Utilize your ability to be flexible and mobile in your business to visit or work from various areas. Additionally, you have the option to strategically schedule your holidays or breaks to coincide with information security events or destinations that capture your attention. Additionally, you can utilize your	(Burton, 2020) (Peeler et al., 2024)

	trip time to acquire knowledge of new languages, customs, and practices that are relevant to the field of information security. Through the act of traveling and engaging in exploration, one has the opportunity to enhance both their personal and professional lives.	
Balance on priorities	One last suggestion for cultivating a global outlook is to effectively manage your priorities and prevent exhaustion. The field of information security can be arduous and tense, particularly when one is consistently confronted with novel risks, problems, and modifications. While staying informed about the worldwide information security situation is crucial, it is equally critical to prioritize your physical and mental health as well as nurture your relationships. One can establish limits, provide time for rest, assign responsibilities to others, and request assistance when necessary. By effectively prioritizing your tasks, you may sustain your love and excitement for information security.	(Koltays et al., 2021) (T. Hunter et al., 2023)

Information Security for an Information Society in Bangladesh

Bangladesh is currently progressing rapidly towards the era of the information society, propelled by a powerful and advantageous force. It is imperative for governments and politicians to recognize the importance of developing a clear vision for the future of this endeavor (Faroque, 2024). Information security is the implementation of measures to reduce the risks associated with the protection of information. Cybersecurity encompasses the safeguarding of information systems and the data they handle, store, and send, to prevent unauthorized access, use, disclosure, disruption, alteration, or destruction (Isakov et al., 2024). This include the safeguarding of personal, sensitive or private, and financial information held in both online and offline styles. To achieve effective information security, a thorough and interdisciplinary strategy is necessary, encompassing individuals, procedures, and technology etc.

Key Findings

Table 3: Key Findings and Themes of the Study

Key Findings and Themes	Description	Reference
Artificial Intelligence (AI) and Machine Learning (ML) Attacks	Research suggests an increasing worry around adversarial attacks on AI/ML systems. Subsequent research should prioritize the development of resilient countermeasures against these threats.	(Chiejina et al., 2024)
Internet of Things (IoT) Security	The widespread adoption of IoT devices poses distinct security challenges. Research should focus on investigating scalable security solutions specifically designed for IoT contexts.	(Kokila & Reddy K, 2024)
Post-Quantum Cryptography	With the advancement of quantum computing, conventional cryptography techniques may become outdated. Future research should give priority to the advancement and application of quantum-resistant algorithms.	(Wong & Bhatia, 2021)
Homomorphic Encryption	This encryption method allows for computations to be performed on encrypted data without the requirement of decryption, therefore preserving the confidentiality of the information. The objective of research should be to enhance the practicality and efficiency of homomorphic encryption.	(Maurya & Joshi, 2024) (Gouert & Tsoutsos, 2024)
User Behavior and Awareness	Human error continues to pose a substantial security risk. To reduce this danger, subsequent investigations should prioritize the development of efficient training programs and awareness efforts.	(McIlwraith, 2021)
Social Engineering Defense Mechanisms	Novel methodologies are required to combat intricate social engineering assaults that manipulate the human mind.	(AkyeşiĿmen & Alhosban, 2024)
Data Privacy Regulations	A continuous study of compliance and its effects on information systems is required due to the changing nature of data privacy rules, such as GDPR.	(Bakare et al., 2024)
Ethical AI in Security	It is of utmost importance to guarantee the ethicality of AI applications in terms of security and prevent any infringement of user rights. Subsequent investigations should focus on ethical principles and frameworks.	(Oladoyinbo et al., 2024) (Fischer et al., 2024)
Technological Innovations	Blockchain technology provides potential answers for ensuring safe transactions and maintaining data integrity. Subsequent investigations should examine its suitability in domains other than cryptocurrencies.	(Adeoye, 2024)
Zero Trust Architecture	Further investigation is necessary to comprehend the implementation difficulties and advantages of this security paradigm, which operates under the assumption of no inherent trust.	(Habbal et al., 2024)

Implication

Policy Formulation in the Information Society

Pekari (2005) defines policy as a collection of concepts and strategies that provide guidance for achieving a specific objective. Thus far, the primary focus in the formulation of information policy has revolved around the appropriate approach for Nation States to handle the distribution of official information, the regulation of information exchange between private and public entities in relation to copyright and privacy laws, and the regulation of the fundamental infrastructure of information and communication technologies (Da Veiga et al., 2020).

Policy Implications for the Information Society

The previous chapter examined the various hypotheses that explain the emergence and significant consequences of the Information Society (Wiggberg et al., 2022). This endeavour fails to present a clear and cohesive depiction of the true nature of the Information Society or how it ought to be regulated. However, it does provide insight into the current matters that are being contested.

Theories regarding the impact of technological changes on society can be categorised into market or labour force based approaches, ranging from basic assumptions to more complex concepts that analyse the economic and social implications at a national level. These theories also acknowledge the growing necessity for an international perspective (Wiggberg et al., 2022). These approaches emphasise the growth of the information sector and the rising significance of knowledge work. They are based on the ideas of the information revolution and the computerization of society, and encompass more comprehensive theories that connect these issues with socio-political aspects. The shifts towards the growing Information Society manifest in various dimensions, including modes of production and productivity, organisational and occupational structures, technological advancements, power redistribution, cultural reformulation, and new scenarios of exclusion. In order to address these aspects, it is necessary to develop policy strategies for the Information Society.

Suggestions And Recommendations for Information Society About Information Security

Bangladesh necessitates dependable physical and information communication technologies (ICTs). Both types of infrastructure work together to provide crucial services in various areas like communications, emergency services, energy, finance, food, government, health, transit, and water. Hence, in order to attain our economic stability and democratic goals, we necessitate dependable physical and digital infrastructure. Physical assets are becoming more reliant on the dependable operation of the digital infrastructure or critical information infrastructure (CII) in order to provide services and carry out commercial activities. As a result, any major disturbance to Critical Information Infrastructure (CII) might have an immediate and severe effect that extends well beyond the Information and Communication Technology (ICT) sector (Oladoyinbo et al., 2024), and hampers a nation's ability to carry out its critical tasks in other sectors. Hence, the security of critical information infrastructure (CIIP) is a responsibility that falls upon every individual (Habbal et al., 2024).

This document is titled "The National Cybersecurity Strategy of Bangladesh". Implementing this step is crucial for safeguarding our cyber domain from potential security threats, dangers, and problems that could jeopardise national security. The Strategy pertains to the nation's national security strategy. The objective of this paper is to establish a unified and comprehensive plan for the year 2021, aimed at ensuring the security and prosperity of Bangladesh. This will be achieved by the coordination of cybersecurity activities among the government, private sector, citizens, and foreign entities.

The National Cybersecurity Strategy provides a structured plan for organising and prioritising actions to mitigate vulnerabilities to our cyberspace or key information infrastructure. In order to accomplish the aforementioned objectives, this Strategy substantially enhances the prominence of cybersecurity within our governments and establishes explicit roles and duties. Recognising the mutual susceptibility to cyber threats, this Strategy also necessitates a collaboration between the public and private sectors to address the possible vulnerability of privately owned vital infrastructures in the banking, utilities, and telecommunications sectors to cyber-attacks.

Furthermore, we acknowledge that cybersecurity is a worldwide problem that requires genuinely global solutions. Hence, we pledge to actively participate in regional and worldwide collaborations to develop effective solutions for tackling the cybersecurity issue, irrespective of the nature of the threat (Rashid et al., 2021). Consequently, we are presenting this Strategy based on the Pillars of the International Telecommunication Union's Global Cybersecurity Agenda (GCA). The Global Cybersecurity Alliance (GCA) has five key strategic pillars and seven aims aimed at fostering collaboration among essential stakeholders in combating cyber threats. Our objective is to assist the GCA in establishing itself as the primary framework for establishing a secure and protected information society.

CONCLUSION

The Information and Communication Technology Division (ICTD) effectively addresses the increasing disparity in access to digital technology across the country. The digital divide has been widening among various demographic groups, including gender, urban and rural areas, socioeconomic status, literacy levels, and social and corporate sectors. This study aims to demonstrate the effective utilization of digital opportunities in order to bridge gaps and ensure the secure availability of information to the information society (Rodríguez-Abitia et al., 2020). The researcher has discovered a comprehensive and practical information security manual that encompasses all crucial aspects of information security. This manual is suitable for government agencies to implement in order to safeguard their systems and information. The researcher aims to provide a collection of information security concepts and measures that can be included into government legislation, regulations, and standards related to information security in Bangladesh (Bhuiyan, 2023). An effective structure and comprehensive set of rules will greatly facilitate the accreditation and certification of government systems, ensuring the security of information and promoting an information society. Furthermore, the cyber security ecosystem is a worldwide and dynamic system that encompasses the information infrastructure of both government and private sectors. It involves the interaction of individuals, processes, data, information, and communication technologies. It also takes into account the environment and factors that impact cyber security. In order to enhance its presence in the ICT industry, as evidenced by its 'Digital Bangladesh' initiative, Bangladesh must priorities cyber security (Rashid et al., 2021). This is crucial to maintain its appeal and competitiveness as a destination for companies currently operating or planning to establish their businesses in Bangladesh.

Limitations of the Study

This research is comprehensive, however, it does possess numerous limitations that require attention. Initially, the PRISMA-based methodology, being a robust method for topic modeling, may not completely distinguish between different themes (Rashid et al., 2021). This is particularly accurate in circumstances where the topics are strongly interconnected or coincide with one other. It is likely that this will result in a lack of precision in the identification of subjects. In the following analysis, our survey was limited to examining publications written in the English language that were documented by the most esteemed datasets. The study was not conducted due to time constraints, as the concepts of information society and information security are extensive. The primary weakness of this study is its reliance solely on secondary sources. The analysis relied on the data provided by the ICT division and new IT-related articles. Therefore, the assurance of data reliability can be achieved. As information is constantly evolving, some of it may become outdated owing to updates in knowledge and data.

Future Directions

The field of information security is characterized by its dynamic and multifaceted nature. Given the rapid pace of technological advancements and the ever-evolving landscape of threats, it is imperative to engage in continuous research endeavors in order to devise resilient and flexible security protocols (Bhuiyan, 2017). The present systematic review, conducted in accordance with the PRISMA framework, aims to shed light on key areas that warrant further investigation. The ultimate objective is to ensure the maintenance of secure information systems within the context of an increasingly information-driven society. In the future, it is anticipated that conceptual research models such as the Technology Acceptance Model (TAM), Theory of

Planned Behavior (TPB), Theory of Reasoned Action (TRA), and Unified Theory of User Acceptance of Technology (UTUAT) will be relevant and suitable for investigating this particular research domain (Amin et al., 2024).

Conflict of Interest

The authors of this research paper affirm that there are no conflicts of interest present in the process of conducting and publishing this study. As of now, no external financial support has been obtained to facilitate the execution of the research project. The authors have declared that they do not have any potential conflicts of interest to disclose in relation to the publication of this work.

Acknowledgement

The researchers express their gratitude to Dr. Md. Rakibul Hoque, Professor, Management Information Systems department, University of Dhaka, located in Bangladesh. His invaluable assistance has greatly contributed to the progress and success of this research endeavor. All authors have made equal contributions to the execution of this study.

REFERENCES

Abdulrasool, F. E., & Turnbull, S. J. (2020). Exploring security, risk, and compliance driven IT governance model for universities: applied research based on the COBIT framework. International Journal of Electronic Banking, 2(3), 237-265. https://doi.org/10.1504/IJEBANK.2020.111438

Adeoye, I. (2024). Securing Retail: Fortifying Supply Chains with Blockchain for Data Integrity and Transaction Security (SSRN Scholarly Paper 4729270). https://doi.org/10.2139/ssrn.4729270

Ahmad, T. (2021). E-Government in Bangladesh: Development and Present State. International Journal of Social Science and Human Research, 4(01). https://doi.org/10.47191/ijsshr/v4-i1-15

Akhter, T., Naz, M., Salehin, M., Arif, S. T., Hoque, S. F., Hope, R., & Rahman, M. R. (2023). Hydrogeologic Constraints for Drinking Water Security in Southwest Coastal Bangladesh: Implications for Sustainable Development Goal 6.1. Water, 15(13), 2333. https://doi.org/10.3390/w15132333

Aksoy, C. (2024). BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS. İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, 7(1), 96–110. https://doi.org/10.33416/baybem.1374001

AkyeşiLmen, N., & Alhosban, A. (2024). Non-Technical Cyber-Attacks and International Cybersecurity: The Case of Social Engineering. Gaziantep University Journal of Social Sciences, 23(1), 342–360. https://doi.org/10.21547/jss.1346291

Al-Mamun, F., Hasan, M. E., Mostofa, N. B., Akther, M., Mashruba, T., Arif, M., ... & Mamun, M. A. (2024). Prevalence and factors associated with digital addiction among students taking university entrance tests: a GIS-based study. BMC psychiatry, 24(1), 322. https://doi.org/10.1186/s12888-024-05737-9

Amin, A., Bhuiyan, M. R. I., Hossain, R., Molla, C., Poli, T. A., & Milon, M. N. U. (2024). The adoption of Industry 4.0 technologies by using the technology organizational environment framework: The mediating role to manufacturing performance in a developing country. Business Strategy & Development, 7(2), e363. https://doi.org/10.1002/bsd2.363

Anu, V. (2022). Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective, 31(4), 466–478. https://doi.org/10.1080/19393555.2021.1922786

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. Computer Science & IT Research Journal, 5(3), Article 3. https://doi.org/10.51594/csitrj.v5i3.859

Bhuiyan, M. R. I. (2017). UNDP-a2i: Citizens' Awareness Survey on E-Service and Service Simplification through the Digital Innovation Fair. Available at SSRN 4341799. https://dx.doi.org/10.2139/ssrn.4341799

Bhuiyan, M. R. I. (2023). The Challenges and Opportunities of Post-COVID Situation for Small and Medium Enterprises (SMEs) in Bangladesh. PMIS Review, 2(1), 141-159. http://dx.doi.org/10.56567/pmis.v2i1.14

Bhuiyan, M. R. I., Akter, M. S., & Islam, S. (2024). How does digital payment transform society as a cashless society? An empirical study in the developing economy. Journal of Science and Technology Policy Management. Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JSTPM-10-2023-0170

Bhuiyan, M. R. I., Uddin, K. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy in the Context of ICT Usages: An Empirical Study in Bangladesh. FinTech, 2(3), 641-656. https://doi.org/10.3390/fintech2030035

Bhuiyan, M. R., & Akter, M. (2024). Assessing the Potential Usages of Blockchain to Transform Smart Bangladesh: A PRISMA Based Systematic Review. Journal of Information Systems and Informatics, 6(1), 245-269. https://doi.org/10.51519/journalisi.v6i1.659

Burns, A. J., Roberts, T. L., Posey, C., & Lowry, P. B. (2019). The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Security-Based Precaution Taking. Information Systems Research, 30(4), 1228–1247. https://doi.org/10.1287/isre.2019.0860

Burton, H. (2020). Conversations About Social Psychology. Open Agenda Publishing. https://doi.org/10.2307/j.ctv22jnnrc

Carmody, P. (2013). A knowledge economy or an information society in Africa? Thintegration and the mobile phone revolution. Information Technology for Development, 19(1), 24-39. https://doi.org/10.1080/02681102.2012.719859

Chen, Y. J. (2017). The method to absorb vibration of uniform mass beam in the action of simple harmonic loads. Mechanics and Architectural Design, 330–335. https://doi.org/10.1142/9789813149021_0045

Chiejina, A., Kim, B., Chowhdury, K., & Shah, V. K. (2024). System-level Analysis of Adversarial Attacks and Defenses on Intelligence in O-RAN based Cellular Networks. Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 237–247. https://doi.org/10.1145/3643833.3656119

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/10.1016/j.cose.2020.101713

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. Commonwealth Law Bulletin, 46(1), 78-109.https://doi.org/10.1080/03050718.2020.1748075

Faroque, S. (2024). Policing green crime in Bangladesh: Challenges for law enforcement, environmental agencies and society [Doctoral, University of Essex]. https://repository.essex.ac.uk/38473/

Fischer, M. T., Metz, Y., Joos, L., Miller, M., & Keim, D. A. (2024). MULTI-CASE: A Transformer-based Ethics-aware Multimodal Investigative Intelligence Framework (arXiv:2401.01955). arXiv. https://doi.org/10.48550/arXiv.2401.01955

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & security, 43, 90-110. https://doi.org/10.1016/j.cose.2014.03.004

Gil-García, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. Government information quarterly, 22(2), 187-216. https://doi.org/10.1016/j.giq.2005.02.001

Gouert, C., & Tsoutsos, N. G. (2024). Data Privacy Made Easy: Enhancing Applications with Homomorphic Encryption (2024/118). Cryptology ePrint Archive. https://eprint.iacr.org/2024/118

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094. https://doi.org/10.1016/j.comnet.2019.107094

Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. Expert Systems with Applications, 240, 122442. https://doi.org/10.1016/j.eswa.2023.122442

Hadad, S. (2017). Knowledge economy: Characteristics and dimensions. Management dynamics in the Knowledge economy, 5(2), 203-225.

Hasnayen, M.E., 2016. Development of a2i Access Information: A Study on Digital Bangladesh. Research Journal of Mass Communication and Information Technology, 2(2), pp.35-42.

Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: How the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. Defense & Security Analysis, 1–35. https://doi.org/10.1080/14751798.2024.2321736

Hunter, T., Seminatore, M., Lindsay, K., & Sanchez, J. (2023). AI AND A SELF-MANAGED ABORTION: CAN CHATGPT PROVIDE ASSISTANCE WHEN NO PHYSICIAN IS PRESENT? Contraception, 127, 110147. https://doi.org/10.1016/j.contraception.2023.110147

Hye, Q. M. A., & Dolgopolova, I. (2011). Economics, finance and development in China: Johansen-Juselius co-integration approach. Chinese Management Studies, 5(3), 311-324.

Isakov, A., Urozov, F., Abduzhapporov, S., & Isokova, M. (2024). ENHANCING CYBERSECURITY: PROTECTING DATA IN THE DIGITAL AGE. Innovations in Science and Technologies, 1(1), Article 1.

Islam, M. A., & Bhuiyan, M. R. I. (2022). Digital Transformation and Society. Available at SSRN: https://ssrn.com/abstract=4604376 or http://dx.doi.org/10.2139/ssrn.4604376

Islam, S. (2021). Selection of Development Projects in Local Government: A Comparative Study of Pathalia and Birulia Union Parishad. Review Pub Administration Manag, 9(6).

Islam, Z., Bhuiyan, M. R. I., Poli, T. A., Hossain, R., & Mani, L. (2024). Gravitating towards Internet of Things: Prospective Applications, Challenges, and Solutions of Using IoT. International Journal of Religion, 5(2), 436-451. https://doi.org/10.61707/awg31130

Ismagilova, E., Hughes, L., Dwivedi, Y.K. and Raman, K.R., 2019. Smart cities: Advances in research—An information systems perspective. International Journal of Information Management, 47, pp.88-100. https://doi.org/10.1016/j.ijinfomgt.2019.01.004

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. Information & Computer Security, 23(3), 246-285. https://doi.org/10.1108/ICS-05-2014-0033

Kokila, M., & Reddy K, S. (2025). Authentication, access control and scalability models in Internet of Things Security–A review. Cyber Security and Applications, 3, 100057. https://doi.org/10.1016/j.csa.2024.100057

Koltays, A., Konev, A., & Shelupanov, A. (2021). Mathematical Model for Choosing Counterparty When Assessing Information Security Risks. Risks, 9(7), 133. https://doi.org/10.3390/risks9070133

Lee, T.D., Park, H. and Lee, J., 2019. Collaborative accountability for sustainable public health: A Korean perspective on the effective use of ICT-based health risk communication. Government information quarterly, 36(2), pp.226-236. https://doi.org/10.1016/j.carbon.2020.02.073

Litvinenko, V., Bowbrick, I., Naumov, I., & Zaitseva, Z. (2022). Global guidelines and requirements for professional competencies of natural resource extraction engineers: Implications for ESG principles and sustainable development goals. Journal of Cleaner Production, 338, 130530. https://doi.org/10.1016/j.jclepro.2022.130530

Maurya, A., & Joshi, M. (2024). Exploring Privacy-Preserving Strategies: A Comprehensive Analysis of Group-Based Anonymization and Hybrid ECC Encryption Algorithm for Effective Performance Evaluation in Data Security. International Journal of Intelligent Systems and Applications in Engineering, 12(13s), Article 13s.

McIlwraith, A. (2021). Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness (2nd ed.). Routledge. https://doi.org/10.4324/9780429281785

Mia, M. N., Mani, L., Rahman, M. M., Milon, M. N. U., & Hossain, R. (2024). Gravitating towards Community Based Tourism (CBT): Community Empowerment and Reducing Poverty in Tourism Sector Development in Bangladesh. International Journal of Religion, 5(6), 848-864. https://doi.org/10.61707/e1zchv24

Mishra, S., & Dhillon, G. (2006, June). Information systems security governance research: a behavioral perspective. In 1st annual symposium on information assurance, academic track of 9th annual NYS cyber security conference (pp. 27-35). New York, USA: ACSAC.

Molla, C., Mani, L., Bhuiyan, M. R. I., & Hossain, R. (2023). Examining the Potential Usages, Features, and Challenges of Using ChatGPT Technology: A PRISMA-Based Systematic Review. Migration Letters, 20(S9), 927-945. https://doi.org/10.59670/ml.v20iS9.4918

Njenga, K. and Brown, I., 2012. Conceptualising improvisation in information systems security. European journal of information systems, 21(6), pp.592-607. https://doi.org/10.1057/ejis.2012.3

Jam, F. A., Singh, S. K. G., Ng, B., & Aziz, N. (2018). The interactive effect of uncertainty avoidance cultural values and leadership styles on open service innovation: A look at malaysian healthcare sector. International Journal of Business and Administrative Studies, 4(5), 208-223.

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., Adebiyi, O. O., Okunleye, O. J., & Ismaila Alao, A. (2024). Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics (SSRN Scholarly Paper 4693987). https://papers.ssrn.com/abstract=4693987

Olson, J. R., Walker, E. R., Chwastiak, L., Druss, B. G., Molfenter, T., Benson, F., Cerrato, A., & Gotham, H. J. (2024). Supporting Implementation Through Online Learning Communities: Lessons Learned From a National Training and Technical Assistance Network. Evaluation & the Health Professions, 47(2), 178–191. https://doi.org/10.1177/01632787241237246

Peeler, A., Nelson, K., Agrawalla, V., Badawi, S., Moore, R., Li, D., Street, L., Hager, D. N., Dennison Himmelfarb, C., Davidson, P. M., & Koirala, B. (2024). Living with multimorbidity: A qualitative exploration of shared experiences of patients, family caregivers, and healthcare professionals in managing symptoms in the United States. Journal of Advanced Nursing, 80(6), 2525–2539. https://doi.org/10.1111/jan.15998

Pekari, C. (2005). The information society and its policy agenda: towards a human rights-based approach. Revue québécoise de droit international, 18(1), 57-74. https://doi.org/10.7202/1069239ar

Poli, T. A., Sawon, M. M. H., Mia, M. N., Ali, W., Rahman, M., Hossain, R., & Mani, L. (2024). Tourism And Climate Change: Mitigation And Adaptation Strategies In A Hospitality Industry In Bangladesh. Educational Administration: Theory and Practice, 30(5), 7316-7330. https://doi.org/10.53555/kuey.v30i5.3798

Prastyanti, R. A., & Sharma, R. (2024). Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India. Journal of Human Rights, Culture and Legal System, 4(2), 354-390. https://doi.org/10.53955/jhcls.v4i2.200

Rashid, Z., Noor, U., & Altmann, J. (2021). Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. Future Generation Computer Systems, 124, 436-466. https://doi.org/10.1016/j.future.2021.05.033

Rendon, J. M., & Rendon, R. G. (2022). Analyzing procurement fraud in the US Navy. Journal of Financial Crime, 29(4), 1297-1317. https://doi.org/10.1108/JFC-09-2021-0207

Riahi, E., & Islam, M. S. (2024). Employees' information security awareness (ISA) in public organisations: Insights from cross-cultural studies in Sweden, France, and Tunisia. Behaviour & Information Technology, 0(0), 1–23. https://doi.org/10.1080/0144929X.2024.2311734

Rodríguez-Abitia, G., Martínez-Pérez, S., Ramirez-Montoya, M. S., & Lopez-Caudana, E. (2020). Digital gap in universities and challenges for quality education: A diagnostic study in Mexico and Spain. Sustainability, 12(21), 9069. https://doi.org/10.3390/su12219069

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & management, 46(5), 267-270. https://doi.org/10.1016/j.im.2008.12.007

Sylwia, P., Barzykowski, K., Tracz-Krupa, K., Cassar, V., & Said, E. (2024). Developing cross-cultural competence of students through short-term international mobility programme. International Journal of Training and Development, 28(2), 169–188. https://doi.org/10.1111/ijtd.12315

Taskeen, & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. Blockchain in Healthcare Today, 7(1). https://doi.org/10.30953/bhty.v7.302

Thakuriah, P.V., Tilahun, N.Y. and Zellner, M., 2017. Big data and urban informatics: innovations and challenges to urban planning and knowledge discovery. In Seeing cities through big data (pp. 11-45). Springer, Cham. https://doi.org/10.1007/978-3-319-40902-3_2

Venkateswaran, R. T., Vadivelu, S., & Krishnan, S. (2022). Long-term orientation of South Asian leadership and organizational competitiveness and survival of Sasken Technologies Limited. South Asian Journal of Business Studies, 11(4), 385-396. https://doi.org/10.1108/SAJBS-11-2019-0208

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. IEEE Access, 8, 227756-227779. doi:10.1109/ACCESS.2020.3045514

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Ware, J., & Healey, I. (2018). Conceptualizing Progress in Children with Profound and Multiple Learning Difficulties. In J. Ware (Ed.), Educating Children with Profound and Multiple Learning Difficulties (1st ed., pp. 1–14). Routledge. https://doi.org/10.4324/9780429487682-1

Weiss, J. (2010). Protecting industrial control systems from electronic threats. Momentum Press.

Wiggberg, M., Gulliksen, J., Cajander, Å., & Pears, A. (2022). Defining digital excellence: Requisite skills and policy implications for digital transformation. IEEE Access, 10, 52481-52507. https://doi.org/10.1109/ACCESS.2022.3171924

Wong, R., & Bhatia, A. S. (2021). Quantum Algorithms: Application Perspective. In N. Kumar, A. Agrawal, B. K. Chaurasia, & R. A. Khan (Eds.), Advances in Information Security, Privacy, and Ethics (pp. 82–101). IGI Global. https://doi.org/10.4018/978-1-7998-6677-0.ch005

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security, 21(1), 115-158. https://doi.org/10.1007/s10207-021-00545-8