Journal of Infrastructure, Policy and Development 2024, 8(8), 6303.
https://doi.org/10.24294/jipd.v8i8.6303

Article

The impact of intellectual property rights and the level of information sensitivity on information security in the United Arab Emirates

Fanar Shwedeh[1,*], Nadia Yas[2], Zeana Abdijabar[3], Najlaa Flayyih[3], Ahmad Fadli[3], Harith Yas[4], Adel Salem Allouzi[5]

[1] City University Ajman, Ajman 18484, U.A.E
[2] College of Law, Umm Al Quwain University, Umm Al Quawain 536, U.A.E
[3] College of Law, Ajman University, Ajman 436, U.A.E
[4] Azman Hashim International Business School, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[5] Law College, Abu Dhabi University, Abu Dhabi 59911, U.A.E
*** Corresponding author:** Fanar Shwedeh, s.fanar@cu.ac.ae

CITATION

Shwedeh F, Yas N, Abdijabar Z, et al. (2024). The impact of intellectual property rights and the level of information sensitivity on information security in the United Arab Emirates. Journal of Infrastructure, Policy and Development. 8(8): 6303. https://doi.org/10.24294/jipd.v8i8.6303

ARTICLE INFO

Received: 9 May 2024
Accepted: 11 June 2024
Available online: 27 August 2024

Abstract: In the rapidly evolving landscape of technological innovation, the safeguarding of Intellectual Property Rights (IPR) emerges as a critical factor influencing economic growth and technological advancement. This study, conducted in the context of organizations operating in the United Arab Emirates (UAE), meticulously explores the intricate dynamics between IPR awareness, enforcement, and their implications for information security practices. The research undertakes a thorough investigation with three primary objectives: a comprehensive examination of IPR awareness, an exploration of the relationship between IPR enforcement and information security practices, and an assessment of the impact of information sensitivity. To achieve these objectives, a sample population of 150 respondents from various sectors was engaged, employing a combination of survey instruments and robust statistical analyses. The findings of the study illuminate a strong positive correlation between IPR awareness and information security practices, underscoring the pivotal role of cultivating IPR awareness among organizations. Furthermore, the enforcement of IPR, intricately connected with a resilient legal framework, regulatory authorities, international agreements, and effective customs and border control measures, is identified as a significant influencer of information security practices. The study employs a statistical model that exhibits a high explanatory power, elucidating approximately 85.9% of the variance in information security practices. In conclusion, the research offers profound implications for organizations, policymakers, and stakeholders in the UAE, advocating for strategies such as education, legal and regulatory support, international collaboration, and robust access control mechanisms to fortify IPR awareness, enforcement, and information security practices. The integration of advanced tools such as the smart PLS software adds depth and reliability to the study's analytical framework, contributing to its comprehensive insights.

Keywords: intellectual property rights; IPR awareness; enforcement of IPR; information security practices; United Arab Emirates; information sensitivity; legal framework; regulatory authorities

1. Introduction

Every nation anticipates that the effect of investments in knowledge and ICTs will be the cornerstones of enhanced productivity, social welfare, and sustained economic growth. This is undoubtedly not the case in every country in the globe, and it also varies from year to year and from one time to the next (Aboelazm, 2022). We cannot hold a nation like Ethiopia, where the percentage of Internet users is 1.1%, to

the same standards as a country like Germany, where the rate is about 83% (Shwedeh et al., 2024). Sadly, this significant technical advancement significantly lessens the impact of network externalities, whether they are knowledge- or technology-related, which is why the term "virtual inequality" is appropriate (Piper, 2028). Put another way, "national features" (such as the population's educational attainment, regulation, and existing infrastructure) have an impact on even the impact of ICTs (Yas et al., 2024). Coming up next are, in a word, the main components impacting the reception of new information and communication technologies, but there are a lot more too:

- Economic factors: Over time, technology will cut prices and reduce distances, providing new chances for the educational phenomena. Factors like GDP size, expected return on investments, implementation time, and risk magnitude play a significant role in amplifying the economic effects.
- Social Factors: In terms of social factors, we think the most crucial ones are inadequate education, resistance to new ideas, and inadequate security of the electronic environment. Even if it is difficult to replace the education sector, insufficient security might be provided by enforcing stronger regulations on data confidentiality;
- An additional variable that may have a little impact on technology availability include the political system, environment, religion, and currently in effect laws.

In one of his exceptional books, Common Wealth: Economics for a Crowded Planet, Jeffrey Sachs, proposed that maintainable improvement in the "time of organizations" depends on the accompanying various components, all approaching from the Data and Correspondence Innovations (EMC, 2014): the universal network of districts through the ICTs to the worldwide governmental issues and culture; the proficient division and distribution of workforce at nearby and worldwide level, through the coordination of movement through the Web; limitless and convenient correspondence ways empowering correspondence between networks at worldwide level; the Data and Correspondence Advancements will play the essential part of giving a stage which will guarantee the obligation, checking and assessment of monetary exercises, clinical consideration as well as other human and hierarchical exercises; the intercession of trade connections among purchasers and venders; building interest-centered networks through the instruments presented by the informal communities present on the Web; schooling and expert preparation with regards to distance learning and long lasting learning training (Khudhair et al., 2019). We can't underestimate the meaning of upgrading the beneficial outcomes of ICTs through different public or neighborhood guidelines, public elements, and nearness or topographical position impacts, even in the tedious and sometimes free course of ICT dissemination on the Web (Harith et al., 2024).

Primary responsibilities for safeguarding intellectual property rights currently, there are three main ways to safeguard intellectual property in the world: patents, copyrights, and commercial secrets. There have also been other applications of intellectual property protection techniques (EMC, 2014):

- Moral-ethical guidelines;
- Administrative actions (such as setting up security services, organising a confidentiality policy, and providing staff training);
- Taking physical precautions, such as securing windows and doors;

- Electromechanical, acoustic, radio-technical, magneto metric, and other technological protective systems;
- Cryptographic techniques (information altered to hide its logical core);
- Employment agreements that contain a clause on termination (requiring workers to keep business secrets private).

The conventional idea of copyright has been challenged by the growth of the Internet, making the protection of intellectual property rights even more important. Resources may be inexpensively copied and widely distributed using online resources. The interests of those who create intellectual property items must be carefully balanced with those of advancing societal creativity and raising public awareness (Khudhair et al., 2019). One of the most hotly debated issues in Internet governance is the restriction of unrestricted copying of content and the preservation of chances to utilise such content (Aboelazm, 2021). When intellectual property rights are not upheld online, scientists and researchers could not profit materially from their work, which might lead to a decline in scientific innovation (Norton, 2011). Unifying national legal frameworks for writers' digital rights is crucial, given the worldwide reach of the Internet. The international convention is the most useful vehicle for bringing legislative frameworks on intellectual property rights together (Yas et al. 2022). It has been demonstrated that traditional means of protecting intellectual property rights are ineffective (Mardani et al., 2020). Thus, technological and software-based measures must be taken to safeguard the rights owners' interests first. Information technologies are developing quickly, necessitating the need for new protective measures (Aboelazm, 2023).

1.1. Information security in the UAE

As per DLA Piper Global Law Firm's publication, Data Protection Laws of the World, the Government Laws of the Unified Middle Easterner Emirates don't determine the degree of control or data safety efforts that should be carried out to forestall the unapproved divulgence of individual data. All things being equal, offenses relating to unapproved or unlawful admittance to data relating to private and delicate monetary data, for example, financial balance or Mastercard subtleties, are the focal point of Articles 2 and 3 of the Cyber Crime Law (Piper, 2018). Meaning to "safeguard the protection of client individual data that they keep up with in their documents whether in electronic or paper structure; and limit admittance to shopper data to prepared and approved staff", the regulation (Provision 3 of the Security of Purchaser Data Strategy) requires organizations, including banks and broadcast communications organizations, to find fitting ways to forestall the unapproved exposure or utilization of client data (Yas and Alkuwaiti, 2023). Drawing from the aforementioned, DLA Piper deduced that, in accordance with the UAE Law's viewpoint, the optimal approach would be to guarantee the implementation of substantial security measures to prevent inadvertent exposure and illicit or unapproved handling of personal data. Cybersecurity is a major worry for Middle Eastern organisations and businesses, according to a Gulf Business News report (Gulf Business News, 2013). The EMC Global Data Protection Index 2014 results show that businesses in the United Arab Emirates paid US$2.8 billion in 2014 for data loss and downtime (EMC, 2014).

Furthermore, according to the survey, the number of corporate assaults has more than doubled from the previous year. Additionally, 2.4 times as many victims of targeted assaults were impacted in 2014 as in 2013 (EMC, 2014). The Development Grid: Examination of Normal Development Score by District and Nation is introduced in Reference section A (Khudhair and Mardani, 2021). The focuses not entirely set in stone by the development of the data protection procedure utilized. The discoveries showed that the UAE is among the most un-mature countries as far as data protection program development out of the 24 nations remembered for the review (EMC, 2014).

1.2. Data protection in the UAE

By and large, UAE data protection laws are not generally so progressed as those in different nations (Yas et al., 2024). There is definitely not an exhaustive or designated security and data protection law in the UAE (Norton Rose Fullbright, 2011). As per the EMC Worldwide Data Protection File 2014, the UAE has the most reduced Data Protection List Development Rank, with a rate score of 0.0% (EMC, 2014). Thus, instead of being represented by a different regulation, certain crook code segments handle data protection and security related matters (Bennett, 2017). A few major guidelines relating to the control and protecting of data and delicate data are given by the UAE Punitive Code (Aboelazm, 2023). For instance, the UAE Punitive Code lays out a legal crime for uncovering private data and distributing individual data that compromises a person's or alternately family's security. Such disclosure is deserving of fines, prison time, or both (Blakeney and Mengistie, 2011). Certain enterprises or concentrated callings, such banking, protection, exchanging, and medication, are likewise represented by extra guidelines well defined for that industry (Hoffman et al., 2015). The sanctioning of UAE Bureaucratic Law 3 of 2013 laying out the National Electronic Security Authority (NESA), Bureau Goal 21 of 2013 on IT Security Guidelines at Central Government parastatals, UAE Administrative Law 5 of 2011 Fighting Cyber Crime, and UAE Bureaucratic 6 of 2010 connecting with Credit Data are the absolute latest advancements including the establishment of laws that apply to such unmistakable areas of data or protection matters. Extra laws, for example, those remembered for the UAE Work Law and UAE Common Code (Sargolzaei and Fateme, 2017), likewise apply to data protection. Notwithstanding, as to the Unified Bedouin Emirates, the Dubai International Financial Centre (DIFC) is the sole specific data protection regulation that directs the handling of individual data. This rule applies to the two people and organizations who work inside the DIFC, one of Dubai's free zones (Al-Bayati et al., 2024). The suggested research model conducted in the context of organizations operating in the United Arab Emirates (UAE), meticulously explores the intricate dynamics between IPR awareness, enforcement, and their implications for information security practices (**Figure 1**).

1.3. Framework of the study

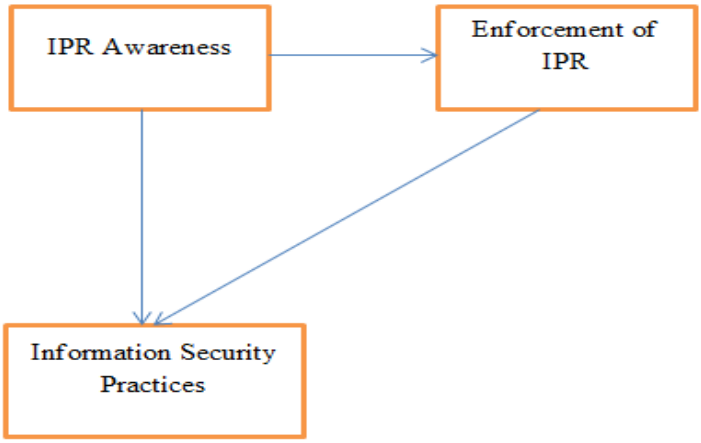

Figure 1. Framework of the study.

2. Literature review

The mediating role of supply chain risk in the logistics and distribution sector was examined by Alshurideh et al. (2023) and offered novel insights for further study, writing, and targeted industries. The suggested research model was subjected to a quantitative research approach combined with a descriptive, causal, and analytical design (Mardani et al., 2020). The research variables were evaluated using a sample of 301 respondents from the management departments of 176 logistics and distribution organizations in Dubai and Abu Dhabi. The results showed that, although supply chain risk had an indirect beneficial influence on the e-supply chain, the impact of information systems was positively correlated with it. The study's scope is restricted to evaluating intermediary supply chain risk. It is advised that future studies examine the effects of SC risk prevention techniques on the E-supply chain. By applying information security policies both internally and externally to improve e-supply chain performance and supply chain risk management, research findings should help communities of practice make better information security decisions in the context of e-supply chains (Sarhan et al., 2023).

Farid et al. (2023) researched how DISM arrangements were applied to practices and execution in college libraries. It additionally takes note of the hardships scholastic libraries have while carrying out these DISM rehearses with regards to strategy (Yas and Shwedeh, 2024). To achieve the review's objectives, a complete assessment of the writing was done. The data was assembled from notable databases, including IEEE Xplore, Emerald Knowledge, ACM Advanced Library, Scopus, Taylor and Francis, ProQuest, Science Direct, Wiley Online Library, Google Researcher, and Library Information Science and Technology Abstracts (LISTA), Library and Information Science Abstracts (LISA), and IEEE Xplore (Khudhair et al., 2021). It involved watchword looking to pick appropriate papers as per the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) norms. A couple of college libraries have made DISM strategies including data security and protection, data protection from malware and social designing, data reinforcement, data security (IS) frameworks, equipment and programming improvement, and staff preparing (Yas, and

Daf, 2024). A couple of libraries have made a framework to shield clients' confidential data from malware, infections, programmers, and social designing. The outcomes showed that since libraries have severe protection and data security rules, the two clients and organizations trust them. Despite the fact that they have laid out DISM arrangements, a few scholastic libraries decided not to acknowledge and apply them in their associations. The DISM strategy on data security and protection, data reinforcement, IS frameworks, equipment and programming updates, and specialized staff help has been bringing on some issues for libraries (Harith et al., 2021). They additionally need to manage financing limitations and administrators' hesitance to embrace new apparatuses and advances like DISM. The DISM strategy was challenging to plan and direct for library experts. Partners, heads, and library experts need to energize the DISM strategy culture in scholarly world to safeguard data security and protection. To shield delicate, confidential data and assets, library experts, officials, heads, and the executives can profit from this concentrate by making and carrying out DISM strategies in their associations or libraries (Aburayya et al., 2022). This paper, which is the first of its sort to assess DISM strategy in college libraries, will be useful to data subject matter experts, partners, and heads (Yas, 2021).

A tentative cybersecurity threat model pertinent to the AEC sector was presented by Mathha et al. (2021). In light of this, threat models are suggested for every stage of the life cycle. An example from the commissioning stage of a building, which incorporates an autonomous robotic system to gather data as a potential countermeasure, is used to demonstrate the viability of the suggested technique (Saeed and Khudhair, 2024). Proposed countermeasure exhibits potential to mitigate some cybersecurity issues encountered during the construction certification and commissioning procedure (Alimour et al., 2024). The findings demonstrate that the presence of extra monitoring robot limitations, such as minimum and maximum distance, enhances the probability of identifying rogue sensors. The illustrated models indicate that during critical stages of building projects, the suggested framework will assist in addressing the safety and cyber security of stakeholders and systems (Harith et al., 2022).

3. Methodology

The research employed a mixed-methods research design, which integrated quantitative and qualitative approaches. Quantitative data were gathered through a structured questionnaire, administered to a representative sample of organizations in the United Arab Emirates (UAE). This survey focused on assessing the level of awareness of intellectual property rights (IPR) and their relationship with information security practices. Additionally, secondary data were collected from government reports and industry sources, providing relevant quantitative information on information security incidents, legal cases, and IPR enforcement in the UAE (Alkashami et al., 2023; Shwedeh et al., 2020; Shwedeh et al., 2022; Shwedeh et al., 2023).

3.1. Sampling of the study

The sample population for this study comprises organizations operating within the United Arab Emirates (UAE). The UAE is home to a diverse range of industries, including but not limited to technology, finance, and healthcare, manufacturing, and government sectors. To ensure a comprehensive understanding of the research topic, the sample population is drawn from these sectors, encompassing both private and public entities. A sample size of the study were 150 respondents by using Stratified Random Sampling, which aimed to ensure representation from various sectors and organization sizes within the UAE (Alkashami et al., 2023; Shwedeh et al., 2020; Shwedeh et al., 2022; Shwedeh et al., 2023). The population was divided into strata or subgroups based on characteristics such as industry, organization size, and geographical location. From each stratum, a proportionate number of samples was randomly selected (Aburayya et al., 2023; Salloum et al., 2023; Shwedeh et al., 2022). This approach was instrumental in capturing the diversity of the population, allowing each subgroup to be adequately represented in the sample.

3.2. Collection of data

Primary Data Collection: In the primary data collection phase, a structured questionnaire was developed and administered to a sample of 150 organizations in the UAE. These surveys aimed to assess the level of awareness and understanding of intellectual property rights (IPR) among the organizations and to investigate the relationship between the enforcement of IPR and information security practices. Survey responses were gathered through interviews and online questionnaires, and they provided valuable insights into the perceptions, practices, and attitudes of organizations regarding IPR and information security.

Secondary Data Collection: In addition to primary data, secondary data were collected from various sources, including government reports, industry publications, and legal documents. These secondary sources provided quantitative information related to information security incidents, legal cases, and the enforcement of IPR in the UAE. This data enriched the research by offering a broader context and historical perspective on the interplay between IPR and information security in the UAE.

3.3. Variables of the study

- Enforcement of Intellectual Property Rights (IPR): This variable represents the degree to which IPR laws and regulations are enforced in the UAE. It can be measured through indicators such as the number of legal actions, penalties imposed, and the effectiveness of IPR enforcement agencies.
- Level of Information Sensitivity: This variable reflects the extent to which information is classified as sensitive or confidential within organizations. It can be measured based on the types of information, data protection measures in place, and access restrictions.
- Level of Information Security Practices: This variable measures the information security measures and practices adopted by organizations in the UAE. It can include indicators such as the use of encryption, access controls, cybersecurity policies, and incident response strategies.

3.4. Tools used for data analysis

3.4.1. Descriptive statistics

In the study, various descriptive statistics were applied to summarize and present the collected data. Measures of central tendency, such as the mean, median, and mode, were calculated to capture the central values of the variables related to intellectual property rights (IPR) awareness, information sensitivity, and information security practices. Additionally, measures of dispersion, including the range, variance, and standard deviation, were computed to assess the spread and variability of the numerical data. Frequency distributions and cross-tabulations were constructed to provide clear insights into the frequency and relationships of categorical data. Various charts and graphs, such as bar charts, histograms, pie charts, and box plots, were used to visualize and convey the findings effectively.

3.4.2. Inferential statistics

In the inferential statistics phase, several techniques were employed to draw conclusions and make inferences from the data. Correlation analysis, specifically Pearson's correlation coefficient, was used to measure the strength and direction of linear relationships between variables, allowing us to explore relationships between IPR awareness and information security practices and other pertinent associations. Regression analysis, both simple and multiple, was conducted to investigate relationships between independent variables (e.g., IPR awareness, enforcement, information sensitivity) and dependent variables (e.g., information security practices), enabling predictions and the assessment of the impact of independent variables.

Integral to these analytical processes was the incorporation of advanced tools like the smart PLS software. This software not only enhanced the efficiency and precision of the statistical analyses but also contributed to the robustness and reliability of the study's findings.

4. Data analysis and finding

4.1. Descriptive statistics

Demographic **Table 1** furnishes a comprehensive depiction of the distribution of participants based on several critical demographic characteristics within the study. Also demographic **Figure 1** furnishes Distribution of participants by gender, age, education level, organization type, and industry.

Table 1. Distribution of participants by gender, age, educational level, organization type, and industry.

		F	P	Mean	S.D
Gender	Male	80	54%	3.26	1.026
	Female	70	46%		
Age (in Years)	18–24	25	17%	3.89	0.996
	25–34	45	30%		
	35–44	30	20%		
	45 and above	50	33%		

Table 1. (*Continued*).

		F	P	Mean	S.D
Level of Education	High School or Less	20	14%	3.96	1.056
	Bachelor's Degree	60	40%		
	Master's Degree or Higher	70	46%		
Type of Organization	Private Sector	90	60%	4.02	0.996
	Public Sector	40	26%		
	Non-profit Organization	20	14%		
Industry	Technology	40	27%	3.39	1.027
	Finance	30	20%		
	Healthcare	20	14%		
	Manufacturing	25	17%		
	Other Industries	35	22%		

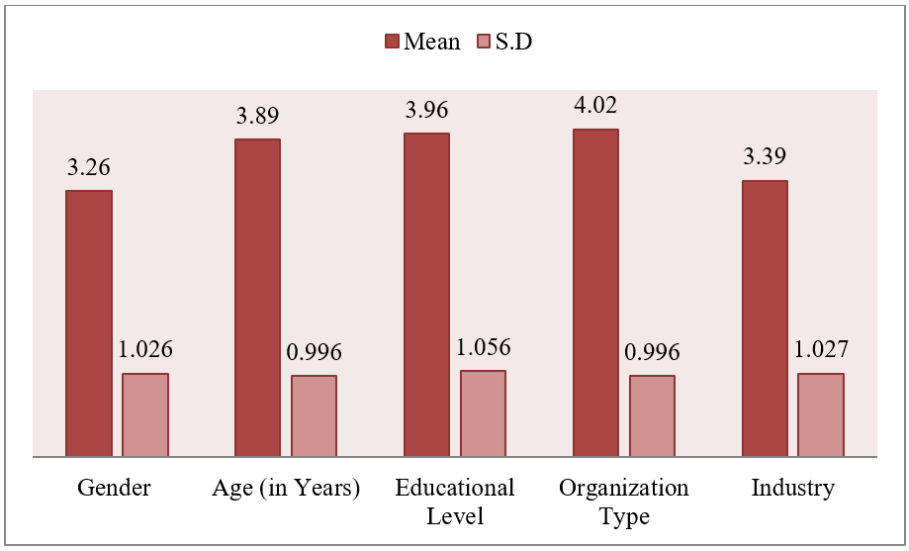

Figure 2. Distribution of participants by gender, age, educational level, organization type, and industry.

4.2. Correlation matrix of level of IPR awareness and enforcement of IPR

Since joining the World Trade Organization (WTO) in 1996, the United Arab Emirates (UAE) has diligently integrated the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) into its intellectual property (IP) framework, ensuring robust protection across its thriving commercial and creative sectors. This integration covers the registration and protection of trademarks, patents, copyrights, industrial designs, and integrated circuit layout designs. The UAE's commitment extends beyond the basic standards, demonstrating dedication to specific areas such as public health, where patents are granted for pharmaceutical products with exceptions for essential medicines to balance innovation and access to affordable healthcare. In agriculture, the protection of inventions related to agricultural chemicals promotes food security and sustainable practices. Additionally, the UAE recognizes and safeguards trade secrets through various legal provisions.

The UAE's adherence to TRIPS is reflected in its comprehensive legal framework, which aligns with international norms such as the Berne Convention, WIPO treaties, and TRIPS itself. For instance, the 1992 Federal Legislation No. 40 revised the UAE's copyright laws, while the Patent Law (Federal Law No. 17 of 1992) and the Trademark Law (Federal Law No. 13 of 1992) further emphasize the UAE's dedication to a robust IP regime. These laws ensure a comprehensive and efficient IP framework, positioning the UAE's economy favorably on the global stage. Looking ahead, the UAE continues to position itself as a leader in shaping the future of IP, both domestically and regionally. Its recognition of TRIPS, combined with a dynamic and forward-thinking approach to innovation, makes the UAE a prime example of leveraging intellectual property for economic and technological advancement.

To fully understand the evolving nature of IPR in the UAE, it is essential to delve into the legal implications of this transformation. The UAE has made strides in updating its IPR laws to align with international standards, particularly in response to the requirements set by the World Trade Organization (WTO) and the World Intellectual Property Organization (WIPO). However, a detailed examination of the specific statutes, such as Federal Law No. (36) of 2021 on Trademarks and Federal Law No. (38) of 2021 concerning Copyrights and Neighbouring Rights, reveals nuances in their application and enforcement. Case law further elucidates how these statutes are interpreted by UAE courts, highlighting areas of both progress and ongoing challenges. For instance, recent rulings have shown a trend towards stricter enforcement of trademark protections, yet there remains variability in judicial decisions regarding copyright infringements (Yas et al., 2024).

Moreover, the regulatory frameworks governing IPR in the UAE are influenced by international agreements such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). This interconnectedness between domestic laws and international standards underscores the complexity of IPR in the UAE. Analysing regulatory frameworks, including the role of the Ministry of Economy and the Emirates Intellectual Property Association, provides insight into the mechanisms of IPR protection and enforcement. The implications of these legal frameworks extend beyond compliance; they impact foreign investment, innovation, and economic growth in the UAE. By expanding the discussion to include these legal dimensions and their practical consequences, this paper will offer a more comprehensive understanding of the current and future state of IPR in the UAE.

The level of IPR awareness is intricately tied to the legal and regulatory framework, international exposure, educational efforts, and the internal policies and practices within organizations. As these factors converge and interplay, they collectively shape the extent to which organizations in the UAE are aware of and appreciate the significance of protecting intellectual property rights.

The enforcement of IPR in the UAE is heavily reliant on a robust legal framework, the capabilities of regulatory authorities, international commitments, and the effectiveness of customs and border control measures. These factors collectively shape the enforcement landscape, influencing the protection of intellectual property rights within the country.

First, focusing on the Level of IPR awareness, it is evident that the factors influencing awareness, such as the Legal and Regulatory Environment (r = 0.789),

International Business Involvement (r = 0.812), Training and Education (r = 0.912), and IPR Policies and Practices (r = 0.896), exhibit strong positive correlations with information security practices. This suggests that organizations with higher IPR awareness tend to have more robust information security practices in place. These positive correlations emphasize the importance of cultivating a culture of IPR awareness, backed by legal and regulatory support, international engagement, educational initiatives, and well-defined policies and practices to enhance information security. Turning to the factors associated with the Enforcement of IPR, correlations also reveal meaningful insights. Legal Framework (r = 0.715), Regulatory Authorities (r = 0.896), International Agreements (r = 0.945), and Customs and Border Control (r = 0.632) exhibit varying degrees of positive correlation with information security practices. These findings underscore the significance of a robust IPR enforcement environment, including well-defined legal structures, competent regulatory authorities, international commitments, and effective border controls, in bolstering information security practices (**Figure 3**).

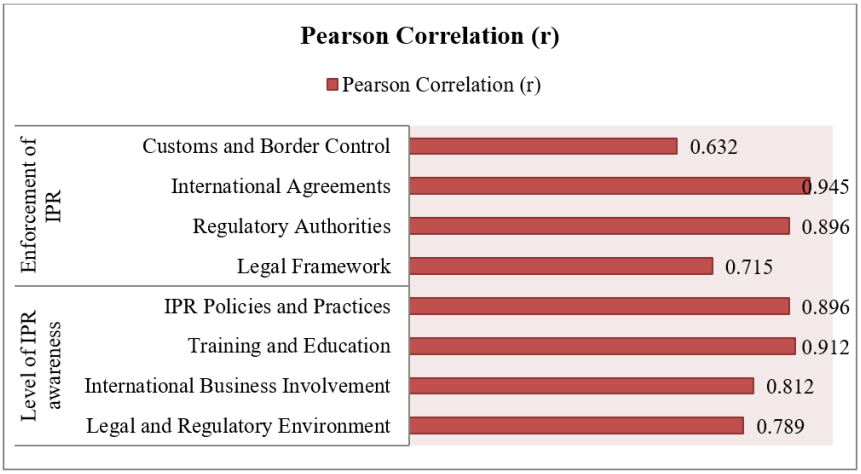

Figure 3. Pearson correlation (r)—relationship between factors and information security practices.

In assessing information security practices within organizational contexts, a multifaceted approach is adopted, integrating various indicators to provide a understanding of the organization's security posture. These indicators encompass key dimensions such as encryption utilization, access control mechanisms, adherence to cybersecurity policies, and the efficacy of incident response strategies. Firstly, encryption employment evaluates the deployment of encryption technologies across organizational systems and communication channels, considering factors such as encryption algorithms and key strength. Secondly, access control scrutiny examines the robustness of access control protocols governing user permissions and system accessibility, including authentication methods and role-based access policies. Thirdly, the evaluation of cybersecurity policies assesses the breadth, clarity, and enforcement of policies governing data management, network security, employee training, and compliance adherence. Lastly, the effectiveness of incident response strategies gauges the organization's readiness to detect, mitigate, and recover from security incidents, encompassing incident detection, response planning, stakeholder coordination, and

post-incident analysis. Integrating these indicators offers a comprehensive depiction of information security practices, elucidating the interconnectedness of various measures in safeguarding organizational assets. The Pearson correlation analysis, as presented in **Table 2**, illustrates the statistical associations between these dimensions and information security practices, underscoring their significance in organizational security frameworks.

Table 2. Pearson correlation (r)—relationship between factors and information security practices.

	Pearson Correlation (r)
Level of IPR awareness	
Legal and Regulatory Environment	0.789
International Business Involvement	0.812
Training and Education	0.912
IPR Policies and Practices	0.896
Enforcement of IPR	
Legal Framework	0.715
Regulatory Authorities	0.896
International Agreements	0.945
Customs and Border Control	0.632

Significance value 0.05*.
Dependent variable: Information security practices.

4.3. Inferential statistics

Table 3, the Model Summary of Variables, offers valuable insights into the statistical model's performance in predicting information security practices. The high *R* Square value of 0.859 indicates that a substantial portion, approximately 85.9%, of the variance in information security practices is explained by these predictors. The Adjusted ***R*** Square of 0.615 considers the model's complexity, providing a slightly more conservative estimate of explained variance. The Std. Error of the Estimate (0.84596) represents the model's accuracy in predicting actual data points.

Table 3. Model summary of variables.

Model Summary				
Model	***R***	R^2	**Adjusted R^2**	**S.E**
1	0.922[a]	0.859	0.615	0.84596

a. Predictors: (Constant), Regulatory Requirements, Data Ownership, Data Classification Policies, Access Control.

Table 4, the ANOVA summary, it assesses the overall significance of the regression model. The significant F-statistic (84.363) indicates that the model as a whole is capable of explaining a statistically significant portion of the variance in information security practices.

Table 4. Anova summary.

ANOVA[a]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	326.361	4	62.363	84.363	0.000[b]
	Residual	152.362	145	0.748		
	Total		149			

a. Dependent Variable: Information security practices.
b. Predictors: (Constant), Regulatory Requirements, Data Ownership, Data Classification Policies, Access Control.

The constant, represented as (Constant), plays a role in the model, and its coefficient is 0.812 with a standard error of 0.215. The associated *t*-value is 3.256, and the significance level (Sig.) is 0.024, indicating that it contributes significantly to the prediction of information security practices. Among the predictor variables, "Regulatory Requirements" has a standardized coefficient (Beta) of 0.055, a *t*-value of 0.812, and a small significance level (Sig.) of 0.003. This suggests that regulatory requirements have a statistically significant, albeit relatively modest, impact on information security practices. "Data Ownership" boasts a more substantial standardized coefficient (Beta) of 0.312, a higher *t*-value of 5.126, and a low significance level (Sig.) of 0.002, indicating a strong and statistically significant influence on information security practices. "Data Classification Policies" exhibit a standardized coefficient (Beta) of 0.108, a *t*-value of 2.678, and a significance level (Sig.) of 0.004. While the influence is less pronounced than data ownership, it remains statistically significant. "Access Control" demonstrates the most robust impact with a standardized coefficient (Beta) of 0.625, a high *t*-value of 6.296, and an exceptionally low significance level (Sig.) of 0.000. Access control is not only highly significant but also has the most substantial influence on information security practices (**Table 5**).

Table 5. Coefficient of determination of the variable.

Coefficients[a]						
Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	0.812	0.215		3.256	0.024
	Regulatory Requirements	0.072	0.092	0.055	0.812	0.003
	Data Ownership	0.412	0.109	0.312	5.126	0.002
	Data Classification Policies	0.211	0.096	0.108	2.678	0.004
	Access Control	0.785	0.097	0.625	6.296	0.000

a. Dependent Variable: Information security practices.

4.4. Primary data analysis

First, it verifies the measurement techniques (outer models). By using the resampling techniques (such as bootstrapping) on 5000 resamples (Vinzi, 2013), In a subsequent phase, the structural model (inner model) is tested. With this advice, the internal consistency of the exterior model was checked first. To determine the extent

to which each indication of the build is strongly linked with its respective latent variable, the initial stage involves evaluating the dependability of the different indicators using their external loadings. As a general rule, accept goods with loads of 0.60 or greater for internal product quality however, it cut criterion for AVE for each measurement construct is 0.50 (**Figure 6**). All constructs of the given model have achieved the criterion of AVE 0.50 after delectation of few of the items from cyber security policies two items has been deleted ISP4 and from Enforcement of IPR two items has been removed ISP3 and ISP4 one item removed IRPR3 from Enforcement of intellectual property rights (**Table 6**).

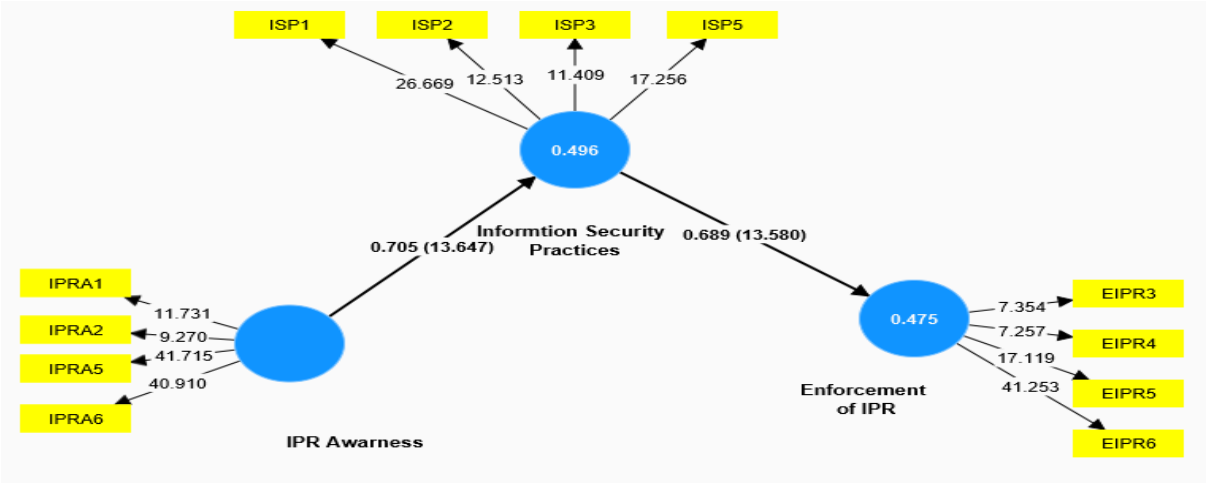

Figure 4. Measurement Model with Standardized Values

Table 6. Measurement model.

Constructs	Items	Factor loading	R-Value	Composite reliability (CR)	AVE
Information Security Practice				**0.861**	**0.560**
	LIS1	0.716			
	LIS2	0.694			
	LIS3	0.758			
	LIS4	0.756			
	LIS5	0.657			
	LIS6	0.760			
Enforcement of Intellectual Property Rights				**0.886**	**0.584**
	IPR1	0.779			
	IPR2	0.726			
	IPR3	0.416			
	IPR4	0.894			
	IPR5	0.903			
	IPR6	0.779			
IPR Awareness			**0.495**	**0.801**	**0.525**
	IPRA1	0.846			
	IPRA2	0.897			
	IPRA3	0.701			

Table 6. (*Continued*).

Constructs	Items	Factor loading	R-Value	Composite reliability (CR)	AVE
IPR Awareness			**0.495**	**0.801**	**0.525**
	IPRA4	0.403			
	IPRA5	0.456			
	IPRA6	0.846			

This led to the conclusion that, as indicated by the CR, the measuring items were correct regarding about their content validity and dependability. The average extracted variance (AVE) was used to evaluate convergent validity including all dormant structures, reflectors predictors, as well as variable loading requirements (Eybpoosh et al., 2011). If any item contains a factor loading that is less than 0.60, it must be removed from the scale to obtain the proper average value for the construct (AVE). An item with factor loading greater than 0.60 can be kept if AVE is larger than 0.50. These criteria were satisfied by the reflected measurement model. Certain items' factor loading ranges from 0.60 to 0.97, supporting convergence of reliability. A discriminating validity test is used in the third stage. Establishes if each model construct differs noticeably from the others. The criteria forner-Larcker and the criterion HTMT are two ways to determine the discriminating validity. **Table 7** is a summary of the Forner-Larcker results:

Table 7. Forner lacker criterion.

	Information Security Practice	Information Security Practice	Information Security Practice	Information Security Practice
Information Security Practice				
Enforcement of Intellectual Property Rights	0.794			
IPR Awareness	0.778	0.804		

When comparing the AVE values with the correlation of square variables (Asyraf and Afthanorhan, 2013), Because the AVE values are larger than the expected square correlations, the existence of discriminating construct validity is also confirmed. **Table 8** also displays the outcome for the HTMT criterion:

Table 8. Heterotrait-monotrait HTMT.

	Information Security Practice	Information Security Practice	Information Security Practice	Information Security Practice
Information Security Practice				
Enforcement of Intellectual Property Rights	0.994			
IPR Awareness	0.878	0.804		
Information Security Practice	0.753	0.659	0.727	

According to Modeling et al. (2015), the heterotrait-monotrait ratios (HTMT) are all less than 0.85, and the upper confidence limits are less than 1. Within the data,

these HTMT results show adequate discriminating validity. These findings provide sufficient assurance that the reflective measurement model fits the data well.

The model's hypotheses were tested, and the convergent and discriminating validity of the measurement model were found to be satisfactory. We examined the impact of each e-Government component on consumer satisfaction, looking at the path coefficients' values and significance (the bootstrapping technique was applied on 5000 subsamples).

In light of the results for the three areas of e-Government use, it can be said that knowledge quality is more significant than service and programme quality in terms of performance. Or to put it another way, accurate information is essential to achieving customer happiness.

4.5. Findings of the study

The findings of the study reveal crucial insights into the relationship between intellectual property rights (IPR) awareness, enforcement of IPR, and their impact on information security practices in the United Arab Emirates (UAE). The analysis demonstrates significant associations between these factors, shedding light on their importance for organizations in the UAE.

- The study indicates a strong positive correlation between IPR awareness and information security practices. Organizations with higher levels of IPR awareness tend to have more robust information security measures in place.
- Factors such as the legal and regulatory environment, international business involvement, training and education, and IPR policies and practices play pivotal roles in shaping IPR awareness among organizations in the UAE.
- Legal and regulatory support, international engagement, educational initiatives, and well-defined internal policies and practices significantly contribute to higher IPR awareness.
- The enforcement of IPR in the UAE is influenced by various factors, including the legal framework, regulatory authorities, international agreements, and customs and border control.
- The study highlights a positive correlation between the enforcement of IPR and information security practices. A robust legal framework, capable regulatory authorities, international commitments, and effective border controls contribute to better enforcement and, in turn, enhanced information security practices.
- Organizations operating in the UAE benefit from strong enforcement mechanisms that safeguard intellectual property rights.
- The study underscores the importance of IPR awareness and effective enforcement mechanisms in strengthening information security practices.
- Access control emerges as a key predictor with the most substantial influence on information security practices. Regulatory requirements, data ownership, and data classification policies also play significant roles.
- The statistical model employed in the study explains approximately 85.9% of the variance in information security practices, indicating its reliability and predictive power.

4.6. Limitations of the study

While the study endeavours to contribute valuable insights into the complex interplay between intellectual property rights, information sensitivity, and information security practices, there are remaining several inherent limitations that impact the interpretation and generalizability of findings. Firstly, the reliance on survey methodology to collect data presents potential limitations, including response biases and self-reporting inaccuracies. Despite efforts to mitigate these biases through robust survey design and data validation techniques, the possibility of social desirability bias or respondent fatigue cannot be eliminated. Consequently, the validity and reliability of results may be influenced to some extent by these methodological considerations.

Secondly, the cross-sectional nature of study design precludes the establishment of causal relationships between variables and limits ability to capture temporal changes over time. While analyses provide valuable insights into the associations between intellectual property rights, information sensitivity, and information security practices, longitudinal studies would be necessary to elucidate the directionality and causality of these relationships more definitively. Furthermore, the generalizability of current findings may be constrained by the specific context of the United Arab Emirates and the characteristics of sample population. While we endeavoured to ensure diversity and representativeness in our sample, it is essential to recognize that results may not fully extrapolate to other organizational settings or cultural contexts.

Additionally, the scope of this study is limited by factors such as sample size, participant demographics, or geographical coverage. While we aimed to maximize the breadth and depth of analyses within practical constraints, the possibility of sampling biases or unmeasured confounding variables cannot be entirely discounted. Despite these limitations, study offers valuable insights into the multifaceted dynamics of intellectual property rights, information sensitivity, and information security practices. By acknowledging these limitations, we aim to provide a more nuanced understanding of the strengths and weaknesses of research findings, thereby facilitating informed decision-making and future research endeavors in this domain.

5. Conclusion

In the context of the United Arab Emirates, this study has explored the intricate relationship between Intellectual Property Rights (IPR) awareness, the enforcement of IPR, and their influence on information security practices. The findings of this research shed light on several critical aspects of the IPR landscape and their implications for organizations and stakeholders in the UAE. The study reveals that a strong positive correlation exists between IPR awareness and information security practices. Organizations that exhibit higher levels of IPR awareness tend to have more robust information security measures in place. This underscores the significance of fostering a culture of IPR awareness within organizations, supported by a conducive legal and regulatory environment, international engagement, education, and well-defined internal policies and practices. Furthermore, the enforcement of IPR is found to be intricately connected to information security practices. A robust legal framework, competent regulatory authorities, international commitments, and effective customs and border control measures collectively contribute to better IPR enforcement.

Consequently, organizations operating in the UAE benefit from enhanced enforcement mechanisms, which safeguard intellectual property rights and reinforce their information security practices.

Recommendation

Based on the study's findings, several recommendations emerge to enhance IPR awareness and enforcement, leading to improved information security practices in the UAE:

- Education and Training: Organizations should invest in IPR education and training programs for their employees to enhance awareness and understanding. These programs should encompass legal aspects, global best practices, and the importance of IPR protection.
- Legal and Regulatory Support: The UAE government and regulatory bodies should continue to provide a robust legal and regulatory framework that promotes and protects IPR. Regular updates and alignment with international standards are essential.
- International Collaboration: The UAE should actively engage in international agreements and collaborations related to IPR, fostering a global environment that supports the protection of intellectual property.
- Customs and Border Control: Customs and border control measures should be continually strengthened to prevent the illegal import and export of counterfeit goods and the infringement of IPR.
- Access Control: Organizations should prioritize access control mechanisms and policies as a crucial element of information security. This includes stringent authentication processes and data access restrictions.

Author contributions: Conceptualization, FS and NY; methodology, ZA; software, NF; validation, AF, HY and ASA; formal analysis, FS; investigation, NY; resources, ZA; data curation, NF; writing—original draft preparation, AF; writing—review and editing, HY; visualization, ASA; supervision, FS; project administration, NY; funding acquisition, ZA. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

Aboelazm, K. (2022). The Role of Digital Transformation in Improving the Judicial System in the Egyptian Council of State. Journal of Law and Emerging Technologies, 2(1), 11–50. https://doi.org/10.54873/jolets.v2i1.41

Aboelazm, K. (2023). The Debatable Issues in the Rule of Law in British Constitutional History and the influence in the Egyptian Constitutions. International Journal of Doctrine, Judiciary and Legislation, 4(2), 521-568.

Aboelazm, K. S. (2021). The constitutional framework for public policy in the Middle East and North Africa countries. International Journal of Public Law and Policy, 7(3), 187. https://doi.org/10.1504/ijplap.2021.118325

Aboelazm, K. S. (2024). Using E-Tenders in the United Arab Emirates to Enhance Transparency and Integrity. Kurdish Studies, 12(1), 91-102.

Aburayya, A., Salloum, S. A., Alderbashi, K. Y., et al. (2023). SEM-machine learning-based model for perusing the adoption of metaverse in higher education in UAE. International Journal of Data and Network Science, 7(2), 667–676. https://doi.org/10.5267/j.ijdns.2023.3.005

Aguboshim, F. C., Ezeasomba, I. N., & Ezeife, J. E. (2019). Sustainable Information and Communication Technology (ICT) for Sustainable Data Governance in Nigeria: A Narrative Review. Journal of Information Engineering and Application (JIEA), 9(5), 15-20. https://doi.org/10.7176/jiea/9-5-02

Alimour, S. A., Alnono, E., Aljasmi, S., et al. (2024). The quality traits of artificial intelligence operations in predicting mental healthcare professionals' perceptions: A case study in the psychotherapy division. Journal of Autonomous Intelligence, 7(4). https://doi.org/10.32629/jai.v7i4.1438

Alshurideh, M. T., Alquqa, E. K., Alzoubi, H. M., et al. (2023). The effect of information security on e-supply chain in the UAE logistics and distribution industry. Uncertain Supply Chain Management, 11(1), 145–152. https://doi.org/10.5267/j.uscm.2022.11.001

Andrés, A. R., & Goel, R. K. (2012). Does software piracy affect economic growth? Evidence across countries. Journal of Policy Modeling, 34(2), 284–295. https://doi.org/10.1016/j.jpolmod.2011.08.014

Asyraf, W. M., & Afthanorhan, B. W. (2013). A comparison of partial least square structural equation modeling (PLS-SEM) and covariance based structural equation modeling (CB-SEM) for confirmatory factor analysis. International Journal of Engineering Science and Innovative Technology (IJESIT), 2(5), 198-205.

Bennett, S. (2017). What is information governance and how does it differ from data governance? Governance Directions, 69(8), 462-467.

Blakeney, M., & Mengistie, G. (2011). Intellectual Property and Economic Development in sub-Saharan Africa. Journal of World Intellectual Property, 14(3/4), 238-264. https://doi.org/10.1111/j.1747-1796.2011.00417.x

Dahu, B. M., Aburayya, A., Shameem, B., et al. (2022). The Impact of COVID-19 Lockdowns on Air Quality: A Systematic Review Study. South Eastern European Journal of Public Health (SEEJPH), 5. https://doi.org/10.11576/SEEJPH-5929

DLA Piper (2018). Data Protection Laws of the World, Full Handbook. (April 2018), p. 1–513. URL: https://www.dlapiperdataprotection.com/index.html (visited on: 17/04/208).

EMC. (2014). Global Data Protection Index. https://www.delltechnologies.com/asset/en-gb/products/data-protection/industry-market/global-data-protection-index-key-findings.pdf, 11-21.

Eybpoosh, M., Dikmen, I., & Talat Birgonul, M. (2011). Identification of Risk Paths in International Construction Projects Using Structural Equation Modeling. Journal of Construction Engineering and Management, 137(12), 1164-1175. https://doi.org/10.1061/(ASCE)CO.1943-7862.0000382

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). Journal of Information Science, 016555152311600. https://doi.org/10.1177/01655515231160026

Gulf Business News. (2013). Cyber Security - The Gulf's Looming Concern. https://link.springer.com/book/10.1007/978-981-15-8735-1

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance. Long Range Planning, 46(1–2), 1–12. https://doi.org/10.1016/j.lrp.2013.01.001

Henseler, J., Ringle, C. M., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hoffman, D. D., Singh, M., & Prakash, C. (2015). The Interface Theory of Perception. Psychonomic Bulletin & Review, 22(6), 1480–1506. https://doi.org/10.3758/s13423-015-0890-8

Kalbasi, A., Alomar, O., Hajipour, M., & Aloul, F. (2007). Wireless security in UAE: A survey paper. In: Proc. of the IEEE GCC Conference.

Khudhair, H. Y., Jusoh, A., Mardani, A., & Nor, K. M. (2019). A conceptual model of customer satisfaction: Moderating effects of price sensitivity and quality seekers in the airline industry. Contemporary Economics, 13(3), 283.

Mantha, B., García de Soto, B., & Karri, R. (2021). Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. Sustainable Cities and Society, 66, 102682. https://doi.org/10.1016/j.scs.2020.102682

Miller Scarnato, J. (2017). The value of digital video data for qualitative social work research: A narrative review. Qualitative Social Work, 18(3), 382–396. https://doi.org/10.1177/1473325017735885

Mostafa, M. M. (2011). A neuro-computational intelligence analysis of the global consumer software piracy rates. Expert Systems with Applications, 38(7), 8782–8803. https://doi.org/10.1016/j.eswa.2011.01.090

Norton Rose Fullbright. (2011). Key data privacy and intellectual property issues in the UAE. https://eprint.iacr.org/2014/374.pdf, 1.

Orgill, G. L., Romney, G. W., Bailey, M. G., et al. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Proceedings of the 5th Conference on Information Technology Education. https://doi.org/10.1145/1029533.1029577

Ravikumar, R., Kitana, A., Taamneh, A., et al. (2023). The Impact of Big Data Quality Analytics on Knowledge Management in Healthcare Institutions: Lessons Learned from Big Data's Application within The Healthcare Sector. South Eastern European Journal of Public Health. https://doi.org/10.56801/seejph.vi.309

Salloum, S. A., Almarzouqi, A., Aburayya, A., et al. (2024). Embracing ChatGPT: Ushering in a Revolutionary Phase in Educational Platforms. In: Artificial Intelligence in Education: The Power and Dangers of ChatGPT in the Classroom. Cham: Springer Nature Switzerland. pp. 171–183.

Salloum, S. A., Almarzouqi, A., Aburayya, A., et al. (2024). Redefining Educational Terrain: The Integration Journey of ChatGPT. In: Artificial Intelligence in Education: The Power and Dangers of ChatGPT in the Classroom. Cham: Springer Nature Switzerland. pp. 157–169.

Salloum, S., Al Marzouqi, A., Alderbashi, K. Y., et al. (2023). Sustainability Model for the Continuous Intention to Use Metaverse Technology in Higher Education: A Case Study from Oman. Sustainability, 15(6), 5257. https://doi.org/10.3390/su15065257

Sargolzaei, E., & Keikha, F. (2017). Examining Software Intellectual Property Rights. International Journal of Advanced Computer Science and Applications, 8(11). https://doi.org/10.14569/ijacsa.2017.081175

Shwedeh, F. (2024). Harnessing digital issue in adopting metaverse technology in higher education institutions: Evidence from the United Arab Emirates. International Journal of Data and Network Science, 8(1), 489–504. https://doi.org/10.5267/j.ijdns.2023.9.007

Shwedeh, F., Aburayya, A., Alfaisal, R., et al. (2022). SMEs' Innovativeness and Technology Adoption as Downsizing Strategies during COVID-19: The Moderating Role of Financial Sustainability in the Tourism Industry Using Structural Equation Modelling. Sustainability, 14(23), 16044. https://doi.org/10.3390/su142316044

Shwedeh, F., Adelaja, A. A., Ogbolu, G., et al. (2023). Entrepreneurial innovation among international students in the UAE: Differential role of entrepreneurial education using SEM analysis. International Journal of Innovative Research and Scientific Studies, 6(2), 266–280. https://doi.org/10.53894/ijirss.v6i2.1328

Shwedeh, F., Hami, N., & Abu Baker, S. Z. (2020). Effect of leadership style on policy timeliness and performance of smart city in Dubai: a review. In: Proceedings of the International Conference on Industrial Engineering and Operations Management; Dubai, UAE; 10-12 March 2020. pp. 917-922.

Shwedeh, F., Salloum, S. S., Aburayya, A., et al. (2024). The Impact of Educating Managers in Adopting AI Applications on Decision Making Development: A Case Study in the UAE. In: Artificial Intelligence in Education: The Power and Dangers of ChatGPT in the Classroom. Cham: Springer Nature Switzerland. pp. 591–603.

Taylor, R. G., & Robinson, S. L. (2015). An information system security breach at First Freedom Credit Union 1: what goes in must come out. Journal of the International Academy for Case Studies, 21(1), 131-138.

Toyo, O. D., & Ejedafiru, F. E. (2016). Utilization of Information and Communication Technologies (ICTs) for Sustainable Economic Development in Nigerian. International Journal of Ergonomics and Human Factors, 12(2), 22-34.

Yas, H., Aburayya, A., & Shwedeh, F. (2024). Education Quality and Standards in the Public School and the Private School-Case Study in Saudi Arabia. In: Artificial Intelligence in Education: The Power and Dangers of ChatGPT in the Classroom. Cham: Springer Nature Switzerland. pp. 563–572.

Yas, H., Alkaabi, A., ALBaloushi, N. A., et al. (2023). The Impact Of Strategic Leadership Practices And Knowledge Sharing On Employee'S Performance. Polish Journal of Management Studies, 27(1), 343–362. https://doi.org/10.17512/pjms.2023.27.1.20

Yas, H., Dafri, W., Sarhan, M. I., et al. (2024). Universities Faculty's Perception of E-learning Tools: Filling the Gaps for Enhanced Effectiveness. In: Artificial Intelligence in Education: The Power and Dangers of ChatGPT in the Classroom. Cham: Springer Nature Switzerland. pp. 573–588.

Yas, N., Al-Bayati, Y., Sarhan, M. I., et al. (2024). Environmental pollution and its relationship to the media and the law: Awareness of the dialectics of the complementary relationship. Research Journal in Advanced Humanities, 5(1). https://doi.org/10.58256/cfrs0347

Yas, N., Dafri, W., Yas, H., & Shwedeh, F. (2024). Effect of e-Learning on Servicing Education in Dubai. In: Artificial Intelligence in Education: The Power and Dangers of ChatGPT in the Classroom. Cham: Springer Nature Switzerland. pp. 623–639.