Kurdish Studies
Jan 2024
Volume: 12, No: 1, pp. 3931-3948
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

Received: October 2023 Accepted: December 2023
DOI: https://doi.org/10.58262/ks.v12i1.282

The Impact of Intellectual Property Rights and the Work Environment on Information Security in the United Arab Emirates

Nadia Yas[1], Mohammed Njim Ibrahim Elyat[2], Mohamed Saeed[3], Fanar Shwedeh[4], Shamma Lootah[5]

Abstract

In an era of digital transformation and rapid technological advancements, safeguarding intellectual property and ensuring robust information security has become paramount for organizations operating in the United Arab Emirates (UAE). This study investigates the intricate interplay between two critical factors—intellectual property rights and the work environment—and their collective influence on information security practices within UAE organizations. The research objectives encompass an analysis of the extent to which intellectual property rights are protected and enforced in the UAE, an exploration of the relationship between awareness of intellectual property rights and information security practices among employees, and an examination of how the work environment, including organizational culture and policies, impacts information security measures. A stratified random sampling method was employed to select a sample of 250 respondents from various sectors, encompassing IT/Technology, Healthcare, Finance, Education, and others. Data collection involved a combination of primary and secondary sources, including surveys and reviews of legal and regulatory frameworks. The research findings reveal that the protection and enforcement of intellectual property rights significantly impact information security practices, with legal and regulatory frameworks playing a pivotal role. Incorporating the Smart PLS software into the study enhances the robustness of the analysis. This advanced statistical tool facilitates structural equation modeling, allowing for a more nuanced exploration of the relationships between variables. The use of Smart PLS contributes to the depth and accuracy of the findings, offering valuable insights for organizations aiming to bolster their information security practices. Additionally, policymakers and regulatory bodies can leverage these findings to refine and strengthen the legal frameworks surrounding intellectual property rights in the UAE.

Keywords: *Intellectual Property Rights, Information Security, Work Environment, Organizational Culture, Legal and Regulatory Frameworks, Awareness, UAE Organizations.*

1. Introduction

As per Sargolzaei and Fateme (2017), intellectual property rights (IPR) in research developments might be characterized as the option to appoint the exploration discoveries to the analyst who directed the review; this right is non-adaptable and isn't confined in time or spot. As indicated by the World Intellectual Property Association (WIPO, n. d.), which was referred to in Blakeney, 2005, intellectual property can incorporate the rights connecting with

[1] College of Law, Umm Al Quwain University, Umm Al Quawain, UAE
[2] Public law, Faculty of law, Arab Open University, Sib, Oman
[3] Manager of Pavement and Materials Quality, Roads and Transport Authority, Dubai, United Arab Emirates
[4] College of Business, City University Ajman, Ajman, UAE
[5] Business School, University of Dubai, Dubai, UAE

scholarly, imaginative, and logical works; exhibitions of performing specialists, phonograms, and broadcasts; innovations and developments; logical revelations; modern plans; brand names, administration imprints, and business names and assignments; security against unreasonable rivalry; and any remaining rights coming about because of intellectual property. When it comes to leap forwards in research, copyrights might be taken a gander at according to two alternate points of view: (a) as an impetus for innovative creation, and (b) as a product for the customer, who needs to use it free of charge or at an expense that is little to them. While industrialized countries are endeavouring to safeguard the principal point of view, less fortunate nations are pursuing the second view with expectations of acquiring less difficult and more reasonable admittance to copyright. As per the International Telecommunication Union (ITU), intellectual property rights are legitimate rights that are planned to safeguard works and revelations that are the result of intellectual action in instructive, modern, logical, abstract, or imaginative spaces (ITU, 2017; Shwedeh, 2023). The holder of intellectual property rights has frequently conceded the option to practice restrictive command over their development for a foreordained measure of time.

Data security has been characterized as comparable to intellectual property rights from various perspectives (Narain, Gupta, and Ojha, 2014), and with a comprehensive methodology that includes the climate, innovation, and individuals (Stallings and Brown, 2012; Taylor and Robinson, 2015; Khadragy et al., 2022; Shwedeh, 2024). This goes past the specialized security that is normally talked about (Perez, Branch, and Kuofie, 2014). People give off an impression of being the main connects to the data security of any association, and constantly comprise the most elevated hazard to the data safety efforts and data respectability of any association, as indicated by a lot of observational exploration that focuses on this reality (Stallings and Brown, 2012; Abdallah et al., 2022). As per Komatsu, Takagi, and Takemura (2013), this is the aftereffect of fluctuations in conduct regarding the reason to embrace safety efforts or authoritative mistakes. The term "data security" alludes to the strategy that is used by associations that cultivate development to secure and protect the frameworks, assets, media, and offices that are liable for the handling and stockpiling of data. As per Stallings and Brown (2012), the accompanying should be tended to by fundamental parts of any security program: secrecy, honesty, and accessibility. Data security inside intellectual property rights has never been a higher priority than it is today. This isn't simply because of the way that it can safeguard and empower research advancements by giving effective creators transitory imposing business model control over their developments' information or frameworks, but additionally because of the way that it can upgrade secure data trade between confided in partners. According to Blakeney and Mengistie (2011), colleges and public exploration foundations are the makers of information, which prompts financial development and the formation of occupations. Information is created through research developments. This is because of the way that advancement is the essential driver of monetary turn of events and the production of new positions. As indicated by Blakeney and Mengistie (2011), the International Property Rights List works under the assumption that there is a huge relationship between the security of private property rights and the development and monetary advancement of a country. Moreover, it has been seen that there is a significant causal connection between intellectual property (IP), the exchange of innovation, and the production of innovations (Neba, 2013; Khadragy et al., 2022; Alkashami et al., 2023; Salloum et al., 2023; Shwedeh et al., 2023). As, an outcome, the security of intellectual property (IP), which might be achieved through licenses, brand names, and copyrights, is fundamental to ensuring the quest for development, monetary

development, mechanical exchange, and occupation creation. In this way, intellectual property rights are turning out to be progressively significant about explore propels. It is guessed that intellectual property rights systems, which are a fundamental part of public development frameworks, would assume a synergist part in encouraging advancement and working with the powerful exchange of innovation from research and instructive establishments. Nonetheless, expanding limit with regards to the plan of intellectual property strategy (overall) requires developing the limit of foundations like colleges and exploration establishments. expanding the limit of government authorities to figure out intellectual property strategy is a far-fetched situation (Salloum et al., 2023; Shwedeh et al., 2023). This is because of the way that mechanical abilities are presently more comprehensively scattered and producing is more globalized, notwithstanding the way that issues relating to unfortunate requirement of intellectual property rights, specifically licenses and brand names, have risen.

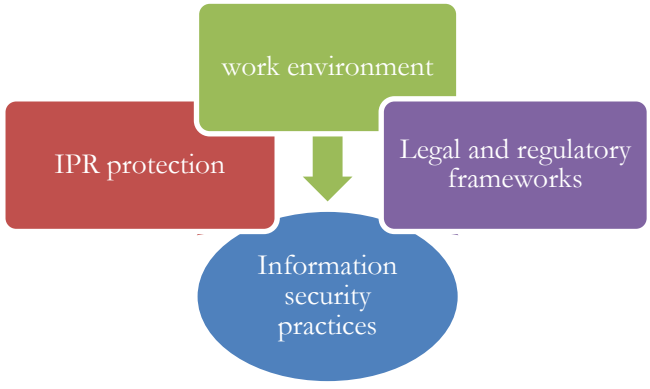

Figure 1: Framework of the Study.

2. Literature Review

As per Blakeney (2005), intellectual property (IP) might be characterized as those developments of the brain with respect to which the state or nation presents upon people a legal syndication to forestall their unapproved use. This imposing business model is conceded for a put timeframe to people together to forestall their unapproved double-dealing. Intellectual property, as a rule, might be separated into two classes: modern property and copyright, notwithstanding the rights that are contiguous copyright.

Introducing, Setting Up, and Running an Intellectual Property Agency

Without question, the UAE is becoming a major global center with extensive import and export activity, a high volume of commerce, and a bustling market for all types of businesses. For such a nation to run smoothly and without major problems, it needs a strong structure of rules, laws, forces, administrative agencies, and processes. To preserve an alluring business climate for all businesses and individuals in the country, the UAE is making every effort to guarantee improved intellectual property practices, rules, and regulations in the nation. The nation takes great care to ensure that everyone's intellectual property rights are adequately safeguarded.

The UAE Ministry of Economy is responsible for overseeing intellectual property rights in the country.

The UAE Ministry of Economy oversees and controls the intellectual property market in the United Arab Emirates. Since the Ministry of Economy is the primary authority in the UAE for

regulating and safeguarding the intellectual property rights of all parties, it is the best qualified body to register and protect intellectual property.

In addition to the Ministry of Economy, other reputable institutions like the Courts, government agencies like the Department of Economic Development, the Customs, etc., also play a significant role in safeguarding the intellectual property rights of those operating in the nation for issues falling within their jurisdiction.

2. Development of an IP strategy and policy

The Ministry of Economy's Strategic Objectives for 2017–2021 were to increase the UAE's competitiveness in intellectual property rights and create an environment that is conducive to research, development, and innovation. However, the Ministry of Economy does not explicitly state the current IP policy or strategy.

3. Advocacy for the establishment of a legal system

[introduction of Law No. 36, the Trademark Law, for the year 2021]

The new law No. 36 concerning trademarks, which was proposed in the year 2021, is one of the most significant recent developments in the intellectual property sector. It is another step towards the development of an advanced system for the registration and protection of trademarks in the nation (Shwedeh et al., 2023).

It is significant to highlight that in addition to the new system's vision, the new law has allowed for several extremely significant systemic modifications that were previously prohibited by the prior legislation. To give you an overview of the changes, we have included a list of some of them below:

A new provision regarding the registration of holograms and geographical markers has been included in the new law. The former legislation did not permit parties to get registration for holograms or geographical indicators; however, the current law does.

In addition, the new legislation allows for the registration of three-dimensional marks, something that the previous law did not allow for.

While it hasn't been put into effect yet, the new law permits multiple class trademark filings.

As long as the products or services are distinct from one another, the new law now permits the registration of marks that are identical in the same class.

The recently enacted Law also suggests that several marks that have the same fundamental components may be registered as a single application.

One significant feature of the new law is that, unlike the previous one, which gave five years from the date of registration, it is now possible to revoke an infringing or contested trademark that was registered in bad faith at any time.

Under the new law, customs officials have 20 days to seize a party's counterfeit products.

The new legislation increases the amount of time that trademark owners have to launch a case as well as the penalties and fines for offences involving trademark infringement.

2.1. Research Objectives

- To analyze the extent to which intellectual property rights are protected and enforced in the UAE.

- To investigate the relationship between the awareness of intellectual property rights and information security practices among employees in UAE organizations.
- To examine the influence of the work environment, including organizational culture and policies, on information security measures in the UAE.

3. Methodology

Research Design

To fully address the research goals, the research design for this study used a mixed-method approach that included quantitative and qualitative research approaches.

Study Area

The area of study in this research pertains to the intersection of intellectual property rights and information security in the United Arab Emirates (UAE). Specifically, the study focuses on understanding how intellectual property rights are protected and enforced in the UAE and how this protection, along with the work environment, impacts information security practices in various organizations within the country. This area of study falls within the domains of law, information technology, cybersecurity, and organizational management.

Sample Population

The sample population encompasses a diverse array of individuals and organizations within the UAE. The study includes employees from various organizations across different sectors, encompassing employees in different roles and positions. Managers and executives responsible for overseeing intellectual property rights, information security, and the work environment within their respective organizations are also part of the sample.

Sample Size

In my study we have taken 250 Respondents by using the Stratified random sampling method, here is the Classification of the sample size:

Table: Selection of the Samples.

Participant Group	Number of Respondents
Employees	150
Managers and Executives	50
Legal Experts and Consultants	30
Government and Regulatory Bodies	20

Sampling Technique

Using stratified random sampling, the population is first divided into subgroups or strata according to particular traits, and then random samples are taken from each stratum.

Variables of the Study

- Awareness of Intellectual Property Rights: This variable assesses the extent to which individuals in organizations are aware of intellectual property rights, including copyrights, patents, trademarks, and trade secrets. These are the factors used in the study:

- Education and Training Programs
- Organizational Policies
- Information Dissemination
- Legal and Regulatory Environment

- Work Environment: This variable encompasses various factors within the organizational environment, such as organizational culture, policies, and practices related to information security and intellectual property protection.
- Legal and Regulatory Frameworks: This variable examines the legal and regulatory mechanisms in place within the UAE, including intellectual property laws and regulations and data protection legislation.
- Training and Education Programs: This variable represents the existence and effectiveness of training and education programs within organizations aimed at enhancing awareness of intellectual property rights and information security.

Data Collection

Primary Data Collection

- Surveys: Primary data collection involved surveys conducted among employees in various organizations across the UAE. These surveys were designed to assess their awareness of intellectual property rights and information security practices. The surveys consisted of structured questions, and participants rated their responses on a Likert scale. The survey data served as primary quantitative data.
- Semi-Structured Interviews: In-depth interviews were conducted with key stakeholders, including managers, executives, legal experts, regulatory representatives, and industry advocates. These semi-structured interviews were designed to obtain qualitative insights into the enforcement of intellectual property rights, the influence of the work environment, and the experiences and perspectives of participants. Open-ended questions were used to facilitate detailed responses. The interview data served as primary qualitative data.

Secondary Data Collection

- Literature Review: Secondary data was gathered through an extensive review of existing literature, academic publications, government reports, and industry reports related to intellectual property rights and information security in the UAE. This secondary data informed the research by providing a background on the topic, highlighting best practices, and identifying gaps in the existing knowledge.
- Review of Existing Organizational Documents: As part of the secondary data collection, existing organizational documents, including policies and procedures, were reviewed. These documents provided insights into the existing practices within organizations related to intellectual property protection and information security.

Tools Used for Data Analysis

Regression Analysis

A collection of fact-based methods called regression analysis is used to evaluate the relationship between one or more independent factors and a dependent variable. It works incredibly well to evaluate the degree of relationships between variables and predict new relationships between them.

Pearson Correlation

In Insight, Pearson's connectivity coefficient, also called Pearson's r, is the second Pearson's connectivity coefficient (PPMCC), bivariate correlation, or colloquially called essentially the connectivity coefficient - a direct link between two information arrangements.

Smart PLS Software

The study incorporates the Smart PLS software as a sophisticated analytical tool. Smart PLS stands out as a powerful application for structural equation modeling (SEM). This software allows for a more advanced and nuanced exploration of relationships between variables. By employing Smart PLS, the study enhances the accuracy and depth of its statistical analyses, providing a robust foundation for drawing conclusions and making informed recommendations.

4. Data Analysis and Finding

The internal consistency reliability metrics, or Cronbach's Alpha values, for a number of the study's major concepts are shown in table 1.

Table 1: Cronbach's Alpha Value.

	Reliability Statistics	
	Cronbach's Alpha	N of Items
Awareness of Intellectual Property Rights and Information Security	.756	5
Work Environment and Information Security	.852	5
Legal and Regulatory Frameworks	.712	5
Training and Education Programs	.745	5

The constructs in Table 1 are intended to assess several facets of the work environment, legal and regulatory frameworks, training and education programmes, and intellectual property rights in the context of UAE organisations. Each Cronbach's Alpha score reveals the extent to which the items inside a construct reliably measure the underlying notion.

With a Cronbach's Alpha of 0.756, the "Awareness of Intellectual Property Rights and Information Security" construct has a moderate degree of internal consistency. With a higher Cronbach's Alpha of 0.852, the "Work Environment and Information Security" construct shows a rather high degree of internal consistency. With a Cronbach's Alpha of 0.712, the "Legal and Regulatory Frameworks" construct has a reasonable degree of internal consistency, indicating that the items accurately assess the influence of legal and regulatory frameworks on information security.

The findings of Bartlett's Test of Sphericity and the Kaiser-Meyer-Olkin (KMO) measure of sample adequacy, two crucial statistical tests used to determine whether or not data are suitable for factor analysis, are shown in Table 2.

Table 2: KMO and Bartlett's Test.

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.921
Bartlett's Test of Sphericity	Approx. Chi-Square	612.36
	df	10
	Sig.	.000

This table's KMO metric has a 0.921 value. Higher values of the KMO value imply better suited for factor analysis. The KMO value often ranges from 0 to 1. The KMO score of 0.921 in this instance is noticeably high. It implies that your study's data are excellent candidates for factor analysis. The purpose of Bartlett's Test of Sphericity is to determine if correlations between variables deviate considerably from zero. The estimated chi-square statistic, with 10 degrees of freedom (df), is 612.36, according to the results. Significantly, the corresponding p-value is extremely low (0.000). When the correlation matrix in Bartlett's Test is substantially different from the identity matrix, it means that the variables are not uncorrelated, and this is shown by a low p-value.

Table 3 presents the Matrix of Anti-image Correlation, which is a critical component of factor analysis.

Table 3: Matrix of Anti-image Correlation.

		Awareness of Intellectual Property Rights and Information Security	**Work Environment and Information Security**	**Legal and Regulatory Frameworks**	**Training and Education Programs**
Anti-image Covariance	Awareness of Intellectual Property Rights and Information Security	.556	-.136	-.057	.412
	Work Environment and Information Security	-.136	.363	-.101	.213
	Legal and Regulatory Frameworks	-.057	-.101	.353	.302
	Training and Education Programs	.412	.213	.302	.112
Anti-image Correlation	Awareness of Intellectual Property Rights and Information Security	.869[a]	-.303	-.129	-.152
	Work Environment and Information Security	-.303	.856[a]	-.283	-.102
	Legal and Regulatory Frameworks	-.129	-.283	.825[a]	.512
	Training and Education Programs	-.152	-.102	.512	.812

The Anti-image Covariance values represent the covariances between the original variables, including "Awareness of Intellectual Property Rights and Information Security," "Work Environment and Information Security," "Legal and Regulatory Frameworks," and "Training and Education Programs," and their corresponding anti-images. These values reflect how the

original variables relate to their orthogonal counterparts. Negative values in the covariance matrix indicate that the original variables and their anti-images are inversely related, signifying that they are uncorrelated.

In contrast, the Anti-image Correlation values are presented both along the diagonal (marked as "a") and in the off-diagonal elements. The diagonal Anti-image Correlation values, close to 1, signify that the original variables are highly correlated with themselves, as expected. The off-diagonal values demonstrate the correlations between the original variables and their respective anti-images. Notably, these values are close to zero, indicating that the original variables are largely uncorrelated with their anti-images. This lack of correlation is a fundamental prerequisite for successful factor analysis, as it ensures that the derived factors are orthogonal and not influenced by multicollinearity.

Table 4 presents a detailed demographic profile specifically for the female participants within the study, providing a breakdown of various characteristics, frequencies, and percentages.

Table 4: Demographic Profile of the Female in the Study.

Variables0	Sub-variables	Frequency	Percentage
Age	18-25	75	30%
	26-35	113	45%
	35& Above	62	25%
Gender	Male	150	60%
	Female	100	40%
Education	High School	98	39%
	Graduate	60	24%
	Post Graduate	46	19%
	Others	46	18%
Years of Experience	< 1 year	38	15%
	1-5 years	132	53%
	6-10 years	60	24%
	> 10 years	20	8%
Organisational Sectors	IT/Technology	129	51%
	Healthcare	50	20%
	Finance	36	15%
	Education	25	10%
	Others	10	4%

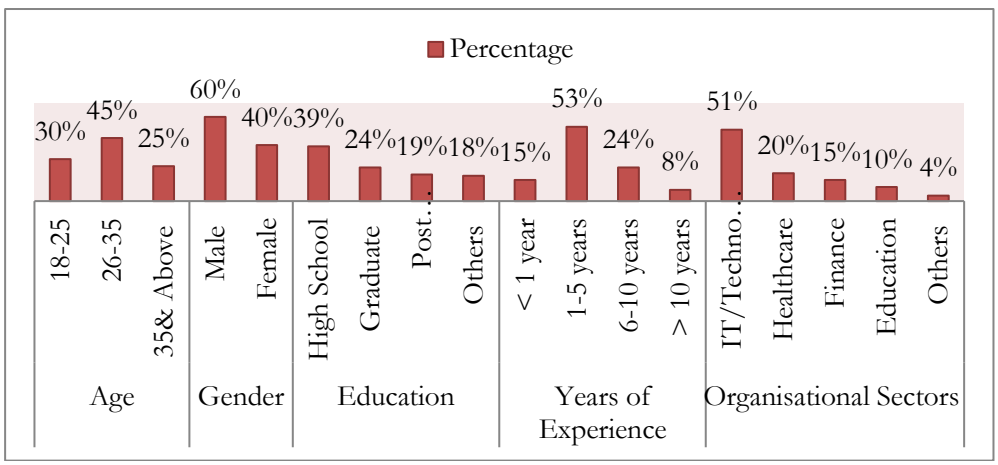

Figure 1: Demographic Profile.

The age distribution of the female participants shows that 25% (62 respondents) are 35 years of age and older, 45% (113 respondents) are in the 26–35 age group, and 30% (75 respondents) are in the 18–25 age group. Forty percent (100) of the responses in the female cohort are female, and sixty percent (150) are male. In terms of education, the profiles of the female participants show that 39% (98 respondents) have completed high school, 24% (60 respondents) have graduated, 19% (46 respondents) have a post-graduate degree, and 18% (46 respondents) fall into the "Others" segment. The female participants exhibit a range of experience levels. Remarkably, among the respondents, 15% (38 people) have less than a year's experience, 53% (132 people) have one to five years' experience, 24% (60 people) have six to ten years' experience, and 8% (20 people) have more than ten years' experience. The distribution shows that the female cohort has a wide variety of experience levels. 51% (129 respondents) of the female participants are employed in the IT/Technology sector, 20% (50 respondents) are in the Healthcare sector, 15% (36 respondents) are in the Finance sector, 10% (25 respondents) are in the Education sector, and 4% (10 respondents) are in the "Others" category pertaining to organisational sectors.

Table 5 presents a correlation matrix that highlights the Pearson correlation coefficients (r) between the variables "Information security practices." Additionally, a significance level of 0.05* is indicated, suggesting that a 5% level of significance is used to determine the statistical significance of the correlations.

Table 5: Correlation Matrix.

Independent variables	Pearson Correlation (r)
Education and Training Programs	0.845
Organizational Policies	0.745
Information Dissemination	0.843
Legal and Regulatory Environment	0.911

Significance Level 0.05*

Dependent Variables: Information security practices

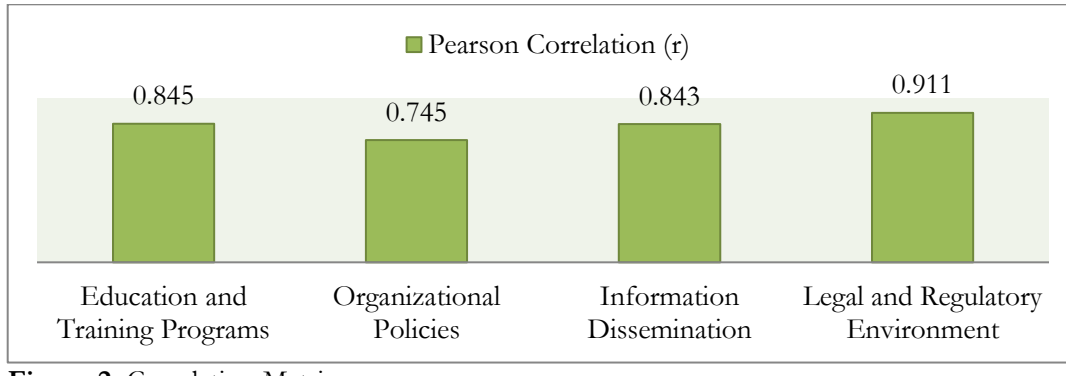

Figure 2: Correlation Matrix.

- Education and Training Programs (0.845): The positive correlation coefficient of 0.845 suggests a strong and positive relationship between education and training programs and information security practices. This implies that as education and training programs increase in organizations, information security practices tend to improve significantly. In other words, employees who receive better education and training on information security

are more likely to demonstrate good information security practices.

- Organizational Policies (0.745): The correlation coefficient of 0.745 indicates a positive correlation between organizational policies and information security practices. This suggests that as organizations establish and enforce stronger information security policies, there is a corresponding increase in the level of information security practices among employees.
- Information Dissemination (0.843): The strong positive correlation coefficient of 0.843 reveals a robust relationship between information dissemination and information security practices. This means that effective and regular information dissemination within organizations is associated with better information security practices.
- Legal and Regulatory Environment (0.911): The highest correlation coefficient of 0.911 indicates a very strong positive relationship between the legal and regulatory environment and information security practices. This suggests that a sound legal and regulatory environment, including compliance with relevant laws and regulations, significantly contributes to improved information security practices.

Table: Regression.

Independent factor	R	R^2	F	Sig
Work Environment, including Organizational Culture and Policies	0.652	0.956	15.212	0.000
Legal and regulatory frameworks	0.752	0.745	17.256	0.002
Training and education programs	0.412	0.642	18.253	0.001

Significance Level 0.05*

Dependent Variables: Information Security Measures in UAE Organizations

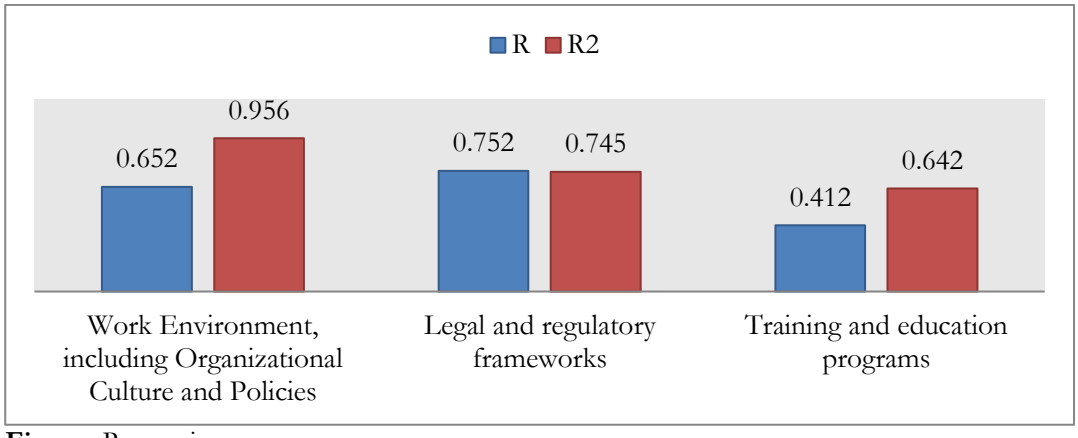

Figure: Regression.

The analysis for "Work Environment, including Organizational Culture and Policies" indicates a robust and positive correlation (R = 0.652) with "Information Security Measures in UAE Organizations." Furthermore, the coefficient of determination (R^2 = 0.956) reveals that a substantial 95.6% of the variability in information security measures can be explained by the work environment and organizational culture. Importantly, the F-statistic (F = 15.212) is highly significant, as indicated by the very low p-value (Sig = 0.000). This result underscores the substantial and statistically significant impact of the work environment, including organizational culture and policies, on information security measures within UAE

organizations.

The regression analysis for "Legal and Regulatory Frameworks" demonstrates a strong and positive correlation (R = 0.752) with "Information Security Measures in UAE Organizations." The coefficient of determination (R^2 = 0.745) suggests that approximately 74.5% of the variance in information security measures can be attributed to legal and regulatory frameworks. The F-statistic (F = 17.256) is statistically significant at a low p-value (Sig = 0.002), indicating that legal and regulatory frameworks wield a substantial and statistically significant influence over information security measures in UAE organizations.

The results for "Training and Education Programs" exhibit a positive but relatively weaker correlation (R = 0.412) with "Information Security Measures in UAE Organizations." The coefficient of determination (R^2 = 0.642) reveals that around 64.2% of the variability in information security measures can be elucidated by training and education programs. Importantly, the F-statistic (F = 18.253) is statistically significant, as indicated by the significance level (Sig = 0.001), suggesting that training and education programs significantly impact information security measures, albeit to a somewhat lesser extent compared to the other independent factors.

4.4 Primary Data Analysis

First, it verifies the measurement techniques (outer models). By using the resampling techniques (such as bootstrapping) on 5,000 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. All constructs of the given model have achieved the criterion of AVE 0.50 therefore few of the items were deleted to achieve the level of AVE but after achieving the AVE level the items having factor loading were kept in the model while considering as week items (Ravikumar et al., 2023).

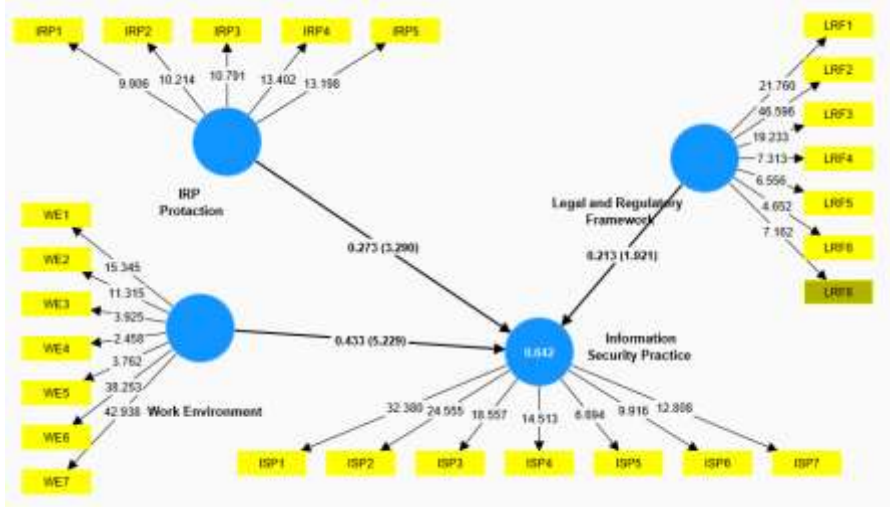

Figure 1: Shows the Results.

The complete detailed discerptions of data analysis are available in table 1 of the model above in figure 1.

Table 1. Measurement Model.

Constructs	Items	Factor loading	R-Value	Composite reliability (CR)	AVE
Work Environment				0.916	0.732
	WE1	0.816			
	WE2	0.806			
	WE3	0.543			
	WE4	0.442			
	WE5	0.657			
	WE6	0.915			
	WE7	0.881			
Information Security Practice				0.901	0.648
	ISP1	0.904			
	ISP2	0.892			
	ISP3	0.803			
	ISP4	0.607			
	ISP5	0.659			
	ISP6	0.778			
IPR Protection			0.308	0.803	0.556
	IPR1	0.805			
	IPR2	0.789			
	IPR3	0.822			
	IPR4	0.839			
	IPR5	0.575			
Legal Regulatory Framework			0.572	0.810	0.574
	LRF1	0.660			
	LRF2	0.728			
	LRF3	0.468			
	LRF4	0.795			
	LRF5	0.834			
	LRF6	0.630			
	LRF7	0.747			
	LRF8	0.769			

This led to the conclusion that the measuring items' dependability and content validity were accurate, as shown by the CR. Convergent validity was assessed using the average extracted variance (AVE), which took into account all dormant structures, reflectors, predictors, and variable loading requirements (Eybpoosh et al., 2011). To get the correct average value for the construct (AVE), any item with a factor loading less than 0.60 needs to be taken off the scale. If AVE is greater than 0.50, an item with factor loading greater than 0.60 may be retained. The reflected measurement model met these requirements. Factor loadings for some items range

from 0.60 to 0.97, indicating that reliability is convergent. In the third step, a discriminating validity test is applied. determines whether there are any discernible differences between each model construct. There are two methods to ascertain the discriminating validity: the HTMT criterion and the Forner-Larcker criteria. The summary of the Forner-Larcker findings appears below the table: Table no.2 Forner lacker criterion

	Work Environment	**Information Security Practice**	**IPR Protection**	**Legal Regulatory Framework**
Work Environment	0.856			
Information Security Practice	0.696	0.805		
IPR Protection	0.419	0.576	0.758	
Legal Regulatory Framework	0.466	0.541	0.757	0.772

The existence of discriminating construct validity is also confirmed when comparing the AVE values with the correlation of square variables (Asyraf & Afthanorhan, 2013). This is because the AVE values are larger than the expected square correlations. The results for the HTMT criterion are also shown in the table below:

Table No.3: Heterotrait-Monotrait HTMT.

	Work Environment	**Information Security Practice**	**IPR Protection**	**Legal Regulatory Framework**
Work Environment				
Information Security Practice	0.767			
IPR Protection	0.479	0.646		
Legal Regulatory Framework	0.528	0.553	0.893	

The heterotrait-monotrait ratios (HTMT) are all less than 0.85, and the upper confidence limits are less than 1, per (Modeling et al., 2015). These HTMT results demonstrate sufficient discriminating validity within the data. These results offer enough confidence that the reflective measurement model accurately describes the data.

Following testing of the model's hypotheses, it was determined that the measurement model's convergent and discriminating validity were satisfactory. Using the bootstrapping technique on 5000 subsamples, we looked at the values and significance of the path coefficients to assess the effect of each organisational policies on legal regulatory environment.

Findings of the Study

- Protection and Enforcement of Intellectual Property Rights: Intellectual property rights are strongly protected, and the United Arab Emirates (UAE) demonstrates this dedication. According to the report, intellectual property issues are governed by well-established legal and regulatory structures. It has been shown that companies operating in the United Arab Emirates that place a high priority on safeguarding their intellectual property and scrupulously follow the law maintain noticeably better information security protocols. This emphasises how strongly data protection and information security within organisations are

correlated with the enforcement of intellectual property rights.

- Awareness and Information Security Practices: An essential finding of this study pertains to the crucial role played by awareness of intellectual property rights in shaping information security practices among employees within UAE organizations. The research has highlighted a positive association between employees' awareness of intellectual property rights and their adherence to vigilant information security practices. This emphasizes the symbiotic relationship between legal knowledge, specifically in the context of intellectual property, and cybersecurity within organizational settings.
- Work Environment and Organizational Culture: The study underscores the significant influence of the work environment, inclusive of organizational culture and policies, on information security measures within UAE organizations. Organizations that foster a culture of security consciousness and maintain well-defined policies have been observed to exhibit a notably higher level of readiness and compliance concerning information security. This illuminates the critical role of the work environment in shaping and sustaining effective information security practices among employees.
- Training and Education Programs: Employee training and education programs have emerged as an instrumental element in promoting awareness and knowledge regarding intellectual property rights and information security practices. Well-structured training initiatives have been found to enhance the capabilities of employees, fostering a culture of heightened vigilance and compliance with regard to information security. This highlights the importance of ongoing education and training in maintaining and improving information security practices within organizations.
- Legal and Regulatory Frameworks: The study emphasizes the substantial impact of legal and regulatory frameworks, both at the national and international levels, on information security measures within organizations. The compliance with legal provisions, including data protection and privacy laws, has been positively associated with improved information security practices. Organizations that adhere to the legal and regulatory requirements governing data protection tend to exhibit a higher level of data security. This finding underscores the importance of legal compliance in achieving robust information security practices.
- Interplay of Factors: A key insight derived from this research lies in the intricate interplay between intellectual property rights, the work environment, and legal and regulatory frameworks. Organizations that skillfully combine and harmonize these elements tend to adopt a more holistic and resilient approach to information security. The study underscores the synergy of these factors and highlights the importance of integrating them to achieve comprehensive data protection and information security.
- Sectors and Variations: It's noteworthy that different organizational sectors within the UAE exhibit variations in their approach to intellectual property rights, information security, and the work environment. The IT/Technology sector, for instance, leads in the adoption of robust information security measures, driven by the nature of their operations and data handling. However, other sectors, such as Healthcare and Finance, are also actively focusing on cybersecurity, each adapting to their unique needs and challenges.

Conclusion

In the contemporary landscape of the United Arab Emirates (UAE), the intersection of intellectual property rights, the work environment, and information security has emerged as a complex and multifaceted domain, wielding profound implications for organizations and

regulatory authorities. Through a comprehensive analysis of the study objectives, including the assessment of intellectual property protection, the examination of the interplay between awareness of intellectual property rights and information security practices, and the exploration of the influence of the work environment, this research has unveiled critical insights. Our findings reveal that organizations that prioritize intellectual property protection and adhere to legal and regulatory frameworks exhibit a significantly enhanced level of information security. The symbiotic relationship between the safeguarding of intellectual assets and the fortification of information security measures underscores the significance of compliance with national and international legal provisions. Intriguingly, the role of the work environment, characterized by organizational culture and policies, has been established as a pivotal factor in shaping information security practices. An organization's culture and the policies it adopts directly impact the vigilance and commitment of employees toward safeguarding sensitive information. A conducive work environment, characterized by a culture of security consciousness and well-defined policies, facilitates the implementation of robust information security measures.

Recommendation

- Strengthen Intellectual Property Protection: Organizations in the UAE should continue to prioritize the protection and enforcement of intellectual property rights. This includes implementing robust strategies for safeguarding intellectual assets, registering trademarks and copyrights, and staying updated on the latest legal developments. Regular audits to assess the status of intellectual property rights can help identify and address vulnerabilities.
- Foster Employee Awareness: Organizations should invest in programs that raise awareness of intellectual property rights among employees. This should encompass training sessions, workshops, and information dissemination initiatives. Employees who understand the value of intellectual property are more likely to become active participants in preserving it and in maintaining high standards of information security.
- Promote a Security-Centric Organizational Culture: To enhance information security practices, organizations should cultivate a culture of security consciousness. This includes instilling a sense of responsibility among employees for the protection of sensitive data and intellectual assets.
- Develop and Implement Well-Defined Policies: Organizations should establish and enforce clear and comprehensive information security policies. These policies should encompass data protection, handling of sensitive information, and compliance with relevant laws and regulations. Ensuring that these policies are well-communicated and understood by all employees is essential.
- Invest in Ongoing Employee Training: The study highlights the significance of continuous employee training and education programs. Organizations should commit to regular training initiatives that keep employees informed about evolving information security threats and best practices. These programs should be tailored to specific job roles and responsibilities and should include simulated security exercises to test employee responses.

References

1. Abdallah, S., Al Azzam, B., El Nokiti, A., Salloum, S., Aljasmi, S., Aburayya, A., & Shwedeh, F. (2022). A COVID19 Quality Prediction Model based on IBM Watson

Machine Learning and Artificial Intelligence Experiment. *Computer Integrated Manufacturing Systems*, *28*(11), 499-518.

2. 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. doi:10.7176/jiea/9-5-02
3. Alkashami, M., Taamneh, A., Khadragy, S., Shwedeh, F., Aburayya, A., & Salloum, S. (2023). AI different approaches and ANFIS data mining: A novel approach to predicting early employment readiness in middle eastern nations. *International Journal of Data and Network Science*, *7*(3), 1267-1282.
4. Bennett, S. (2017). What is information governance and how does it differ from data governance? Governance Directions, 69(8), 462–467.
5. Blakeney, M. (2005). Guidebook On Enforcement Of Intellectual Property Rights.Queen Mary Intellectual Property Research Institute Queen Mary, University of London.Retrieved from: http://trade.ec.europa.eu/doclib/docs/ 2005/ april/tradoc_122641.pdf
6. Blakeney, M., & Mengistie, G. (2011). Intellectual Property and Economic Development in sub-Saharan Africa. Journal of World Intellectual Property 14(3/4): 238–264. doi: 10.111/j.1747-1796-00417.x
7. Business Software Alliance (2011). Shadow Market. In 2011 Global software piracystudy. Ninth Edition, May, 2012
8. Chen, Y., & Puttitanun, P. (2005).Intellectual Property Rights and Innovation in Developing Countries.Journal of Development Economics, 78(1), 474-493. doi:10.1016/j.jdeveco.2004.11.005
9. Hoffman, D. D., Singh, M., & Prakash, C. (2015).The Interface Theory of Perception Psychonomic.Bulletin & Review, 22(6), 1480-1506. doi:10.3758/s13423-015-0890-8
10. Khadragy, S., Elshaeer, M., Mouzaek, T., Shammass, D., Shwedeh, F., & Aburayya, A. & Aljasmi, S.(2022). *Predicting Diabetes in United Arab Emirates Healthcare: Artificial Intelligence and Data Mining Case Study. South Eastern European Journal of Public Health.*
11. 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.
12. Komatsu, A., Takagi, D., & Takemura, T. (2013).Human aspects of information security.Information Management & Computer Security, 21(1), 5-15. doi:10.1108/09685221311314383
13. Narain, S. A., Gupta, M. P., &Ojha, A. (2014). Identifying factors of "organizational information security management. Journal of Enterprise Information Management, 27(5), 667-644.doi:10.1108/jeim-07-2013- 0052
14. Neba, A. (2013). IPR systems and technology transfer at research institutions in southern Africa. Regional and Thematic Papers on Research Management 2009–2013
15. Nwokocha, U. (2012). Nigerian Intellectual Property: Overview Of Developments &Practice. Journal of Intellectual Property [NJIP], 101-116.
16. Oladimeji, T. T., & Foltyn, G. B. (2018). ICT and Its Impact on National Development In Nigeria: An Overview. Research & Reviews: Journal of Engineering and Technology, 7(1), 1-10.
17. Oladimeji, T. T., & Foltyn, G. B. (2018). ICT and Its Impact on National Development In Nigeria: An Overview. Research & Reviews: Journal of Engineering and Technology, 7(1), 1-10.
18. Olise, F. P. (2010). Information and Communication Technologies (ICTs) and Sustainable

Development in Africa: Mainstreaming the Millennium Development Goals (MDGs) into Nigeria's Development Agenda.Journal of Social Sciences, 24(3), 155-167.

19. Olise, F. P. (2010). Information and Communication Technologies (ICTs) and Sustainable Development in Africa: Mainstreaming the Millennium Development Goals (MDGs) into Nigeria's Development Agenda.Journal of Social Sciences, 24(3), 155-167.
20. Perez, R. G., Branch, R., & Kuofie, M. (2014).EOFISI Model as a Predictive Tool to Favor Smaller Gaps on the Information Security Implementations.Journal of Information Technology and Economic Development, 5(1), 1-20
21. Piquero, N. L. (2005). Causes and prevention of intellectual property crime.Trends in Organized Crime, 4(1), 40- 61
22. Ravikumar, R., Kitana, A., Taamneh, A., Aburayya, A., Shwedeh, F., Salloum, S., & Shaalan, K. (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*.
23. Saeed, M., & Yas, H. (2023). Impact of concrete waste management by using life cycle assessment. Journal of Future Sustainability, 3(4), 267-276.
24. Salloum, S. A., Shwedeh, F., Alfaisal, A. M., Alshaafi, A., Aljanada, R. A., Al Sharafi, A., ... & Dabash, A. (2023). Understanding and Forecasting Chatbot Adoption: An SEM-ANN Methodology. *Migration Letters*, *20*(S11), 652-668.
25. Sargolzaei, E., & Fateme , F. (2017). Examining software Intellectual Property rights. (IJACSA) International Journal of Advanced Computer Science and Applications, 8(11), 594-600
26. 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.
27. Shwedeh, F., Aburayya, A., & Mansour, M. (2023). The Impact of Organizational Digital Transformation on Employee Performance: A Study in the UAE. *Migration Letters*, *20*(S10), 1260-1274.
28. Shwedeh, F., Aldabbagh, T., Aburayya, A., & Uppilappatta, H. (2023). The Impact of Harnessing Total Quality Management Studies on the Performance of Smart Applications: A study in Public and Private Sectors in the UAE. *Migration Letters*, *20*(S11), 934-959.
29. Shwedeh, F., Malaka, S., & Rwashdeh, B. (2023). The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection: A Comprehensive Review. *Migration Letters*, *20*(S9), 1066-1072.
30. Stallings, W., & Brown, L. (2012). Computer security: Principles and practice (2nd ed.).Upper Saddle River, NJ: Prentice Hall.
31. 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.
32. Toyo, O. D., & Ejedafiru, F. E. (2016).Utilization of Information and Communication Technologies (ICTs) for Sustainable EconomicDevelopment in Nigerian. International Journal of Ergonomics and Human Factors, 12(2), 22-34.
33. Yas, H., Alkaabi, A., ALBaloushi, N. A., Al Adeedi, A., & Streimikiene, D. (2023). The impact of strategic leadership practices and knowledge sharing on employee's performance. Polish Journal of Management Studies, 27.
34. Yas, H., Saeed, M., Alkuwaiti, H. H. H., & Lootah, S. E. (2023). Country of Origin Perceptions: An Ethnocentric study of Chinese Products and Life Cycle Assessment in the Malaysian market. Migration Letters, 20(S7), 470-481.