SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 4449-4460
Open Access. Online & Print

DOI: 10.5281/zenodo.19010517

EXPLORING THE INFLUENCE OF INTELLECTUAL PROPERTY RIGHTS AND ORGANIZATIONAL CULTURE ON INFORMATION SECURITY MEASURES: A STUDY ON CORPORATE RISK MANAGEMENT

Balaji AK[1] and Nazim Sha S[2*]

[1]Research Scholar, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamilnadu, India, 603203
[2]Assistant Professor, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamilnadu, India, 603203*

Received: 01/02/2026
Accepted: 10/02/2026

Corresponding Author: Balaji AK, Nazim Sha S
(salimkani4@gmail.com and nazims@srmist.edu.in)

ABSTRACT

This paper looks at how Intellectual Property Rights (IPR) and the organizational culture influence the information security measures within corporate risk management in the Indian context. It analyses the data using SPSS software which involves percentage analysis, regression and correlation between how strong IPR frameworks and a proactive security culture improve information security practices. The results demonstrate that the resultant security success in the organizations with strong IPR and a high-security culture is better, but such problems as employee awareness and policy implementation remain. Some of the recommendations involve better training, communication and incorporation of tougher policies to strengthen the IPR and information security. This study is done from Indian organizations.

KEYWORDS: *Information Security, Intellectual Property Rights, Organizational Culture, Network Security, Corporate Risk Management, Employee Awareness*

1. INTRODUCTION

1.1. Information Security

Information security or briefly put, InfoSec, is the policies and tools created and implemented in a bid to ensure that sensitive business information is not altered, interrupted, destroyed or inspected. There are five broad categories of information security namely: application security, Endpoint security, data security, network security, and cloud security.

Network Security

Network security ensures that computer networks are not abused, attacked, and illegally accessed. In order to ensure the safety of the data transfer, it utilizes such methods as intrusion detection systems, firewalls, or VPNs.

Application Security

Application security is mainly aimed at ensuring that software and applications are secured against vulnerabilities and threats. It will include the use of safe codes, frequent updates or testing to avoid such problems as malware or data attacks.

Data Security

Data security provides security by making sure that information remains confidential, true and cannot be accessed by unauthorized users. It encompasses codes, reserve and safe deposits.

Endpoint Security

Endpoints security guard's single devices like Smartphone and computers that connect to a network. It applies antivirus, access control, and encryption to protect against threats.

Cloud Security

Cloud security aims to protect the data, applications and services stored in the cloud environment. It prevents the attacks of the cloud through encryption, access restrictions, and monitoring.

1.2. Intellectual Property Rights

The law protects inventions, artistic and literary works, designs, names, symbols, and images utilized in trade under the notion of intellectual property rights, or IPR.

Trade secrets, industrial designs, patents, copyrights, trademarks, and geographical indications represent the main types of intellectual property rights.

Patent

New, practical, and non-obvious inventions, such as goods or procedures, are protected by patents. It gives the creator of the invention the only right to produce, use, or market it for a maximum of 20 years.

Copyright

Original works such as music, books, movies, and software are protected by copyright. It gives the creator authority over how their work is utilized, duplicated, or shared.

Trademark

A trademark safeguards brand components that set products or services apart, such as names, logos, or slogans. It helps prevent consumer confusion and maintains brand identity.

Trade Secret

Confidential business data that provides a firm with a competitive advantage is covered by trade secrets. As long as the data is valuable and hidden, protection will continue.

Industrial Design

Industrial design rights safeguard the aesthetic features of a product, such as its colour, form, or pattern. They do not cover the functional aspects of the design.

Geographical Indication (GI)

A GI protects those that originate from a specific region and possess qualities or reputation linked to that location. It ensures only genuine regional products can use the name.

1.3. Organizational Culture

A trade secret is unique commercial information that gives a company a competitive advantage. Data protection will continue as long as it is valuable and concealed. It is the values, attitudes and practices that are shared by the workers to influence their choices and behaviors.

A high level of security concerned culture promotes responsibility, adherence and active risk management. Conversely, a poor culture can result in carelessness, policy opposition, or ignorance, which puts more chances of a security breach in place.

To establish a culture of security being an everyday operational process and considered the responsibility of everyone, leadership dedication

and proper communication are necessary.

1.4 Objective

- To understand the factors affecting the integration of Intellectual Property Rights (IPR) in organizational information security.
- To analyze the connection between demographic variables and the perceived efficiency of information security measures.
- To compare the influence of intellectual property awareness and organizational culture on the effectiveness of information security strategies.
- To identify the challenges organizations, face in aligning IPR and cultural factors with their information security approaches.
- To provide recommendations for enhancing information security based on the findings from the analyses conducted.

The remaining manuscript is as follows: Part 2 clarifies the Literature Review, Part 3 outlines the Research Methodology, Part 4 Focuses on Data Analysis and Interpretation and Part 5 covers the findings, suggestion and conclusion.

2. REVIEW OF LITERATURE

As Del-Real (2025) concludes, information security at best relies on the combining of governance frameworks, legal safeguards and organizational culture. Strong intellectual property rights encourage firms to integrate security controls during corporate risk management, the review reveals, while a supportive organizational culture builds employee awareness of risk and compliance to those controls. The broad view, however, is that aligning IPR governance with a security-oriented culture strengthens corporate risk management and organizational resilience.

W. Lu and L. Wu (2024) have presented a blockchain-based system to safeguard intellectual property rights in the AEC industry's digital environments. The system provides practical potential of design management applications through the protection of IPR, an increase in the level of transparency, cost reduction, and efficiency, with non-fungible tokens and blockchain capabilities, including consensus algorithms and cryptography algorithms.

Using the Critical Events Model, A. Oruc et al. (2024) have introduced a maritime industry-specific cyber security training programme, MarCy. It is made up of eleven elective modules, aimed at seafarers and office employees, to increase awareness of cyber. It has been evaluated by experts and found to be relevant to universities, shipping companies and maritime cyber security training institutions.

F. Wang et al. (2024) have presented an examination of Qualitative logic, functional pathways, and the knowledge graph between components like big data, information security, blockchain organisation, user identification, network trust, and blockchain. Nine secondary dimensions and three basic dimensions of digital identification features for users are constructed by the study.

F. A. Shaikh and M. Siponen (2023) have presented that internal variables are frequently overlooked in IS studies on managers' responses to cybersecurity incidents. According to research using the attention-based approach, large breach costs cause TMT to pay more attention to cybersecurity, which in turn affects their choice to carry out an information security risk assessment (ISRA).

D. Broeders et al. (2023) have presented an examination of national cyberterrorism strategies, international diplomacy, and UN cyber standards procedures among permanent members of the UNSC. The article highlights evolving definitions, risks of misuse by authoritarian regimes, and emphasizes the need for precise language to balance cybersecurity efforts with the protection of global human rights.

The authors have a long-standing issue, as shown by the work of A. Shaikh and M. Siponen (2023), where internal organizational factors like culture, leadership attitudes, and employee awareness, which significantly impact managerial choices, are often overlooked in information security studies.

As M. Alnatheer and S. Nelson (2022) demonstrate, organizations with risk-aware cultures are better able to implement proactive information security measures. These findings reveal that organizational cultures in which individuals assist one another significantly improve information security management system performance Y. Chang & H. Lin, (2018).

Organizational culture is a strong determinant of whether the employees comply with information security policies and risk mitigation practices K. D'Arcy, A. Hovav, and D. Galletta (2021).

As noted by A. Alhogail and S. Mirza (2021), the combination of information security under enterprise risk management frameworks can strengthen the company's robust defense against data breaches.

P. Ifinedo (2020) has emphasized that support from top management and alignment of cultural factors are key elements that determine how well the adoption of information security will be successful over time in companies.

S. Von Solms and R. Von Solms (2020) argued that information security must not be viewed simply as a technical issue but as a corporate governance and risk management concern.

According to J. A. Straub and R. Welke (2019), ensuring protection of intellectual property creates trust in the organization, which in turn helps mitigate the strategic and operational risk resulting from information misuse.

T. Herath and H. Rao (2019) proved that intellectual property rights enforcement leads to a stronger organizational security posture where deliberate breaches of security are avoided.

Emerging economies are not without their challenges to coherence of intellectual property regulations and organizational culture, N. Kshetri (2018) points out it is therefore essential to develop the necessary coherence that might drive enhanced corporate information security practices

2.1. Research Gap

Studies on the effects of the intellectual property rights (IPR) and organization culture on the use of information security measures show important gaps in risk management within corporations. Although the significance of IPR in safeguarding organizational resources is acknowledged, little has been done to investigate the direct connection between corporate culture and the execution and success of information security measures. The connection between IPR policies and the internal cultural values, in particular, their impact on the employee behavioral changes in data security, is little studied. Moreover, the variations in implementing IPR with the security measures in the sector are not well-documented. The importance of addressing these gaps is to come up with better, more culture-based information security strategies as part of the corporate risk management system.

2.2. Statement of Problem

Information security has gained great importance to businesses in the recent years. Most companies are now managing their work with the help of digital tools, which leads to the high risk of data leakage and cyber-attacks. When businesses are gathering information on how they can make their data safe using technical means, they fail to place emphasis on the importance of intellectual property rights and the organizational culture. These two points have the ability to influence the compliance of security regulations. This may result in weak protection systems in case it is not managed appropriately. Consequently, it is heavy to understand how corporate culture and intellectual property rights intersect to increase information security and reduce risks.

3. RESEARCH METHODOLOGY

The term research technique identifies how data is identified and analyzed regarding a particular study topic. This method helps researchers in planning their study and employ the instruments of research that they have chosen to achieve their objectives.

3.1. Data Collection

The research gathers information from primary and secondary sources. A questionnaire was used to get primary data, while several journals, books and websites were used to collect secondary data.

3.2. Sampling Techniques

Random sampling is the sample technique employed. Random sampling is an objective method of gathering responses from a population. Standard observation methods and common recording skills are used in random sampling to get data. It is not necessary for the subjects of the study to possess particular abilities or life experiences in order to provide valuable data. Classification mistakes that may arise in other information gathering methods can also be eliminated by this procedure.

3.3. Sample Size

They gave the questionnaire to a sample of around fifty individuals chosen from the target group.

3.4. Tools Used for Analysis

Tools used for analysis are: Percentage Analysis, Regression and Correlation.

3.5. Hypothesis of the Study

Ho: There is no connection between age and effectiveness of protection and security

H1: There is connection between age and effectiveness of protection and security

Ho: There is no connection between education and effectiveness of protection and security

H1: There is connection between education and effectiveness of protection and security

Ho: There is no connection between job role and

effectiveness of protection and security

H1: There is connection between job role and effectiveness of protection and security

Ho: There is no connection between experience and effectiveness of protection and security

H1: There is connection between experience and effectiveness of protection and security

Ho: There is no correlation between intellectual property awareness (including familiarity, influence, and security awareness) and effectiveness of protection and security.

H1: There is a correlation between intellectual property awareness (including familiarity, influence, and security awareness) and effectiveness of protection and security.

4. DATA ANALYSIS AND INTERPRETATION

4.1. Percentage Analysis

Percentage analysis is a technique used to express a part of a whole as a fraction of 100, providing a clear understanding of the proportion of various components within a dataset. The technique is popular in financial analysis, market research and performance measurement which compare the relative sizes, changes over time and the distribution of various variables.

The formula for calculating a percentage is straightforward:

$$Percentage = \left(\frac{Part}{Whole} \right) \times 100$$

Where $Part$ represents the value of the subset being analyzed, and $Whole$ is the total value from which the subset is derived.

4.1.1. Age

The following table indicates that the percentage analysis of age:

Table 4.1: Age.

Variable	No. of Response	Percentage
18-25	35	70%
26-35	7	14%
36-45	5	10%
46 and above	3	6%
Total	**50**	**100%**

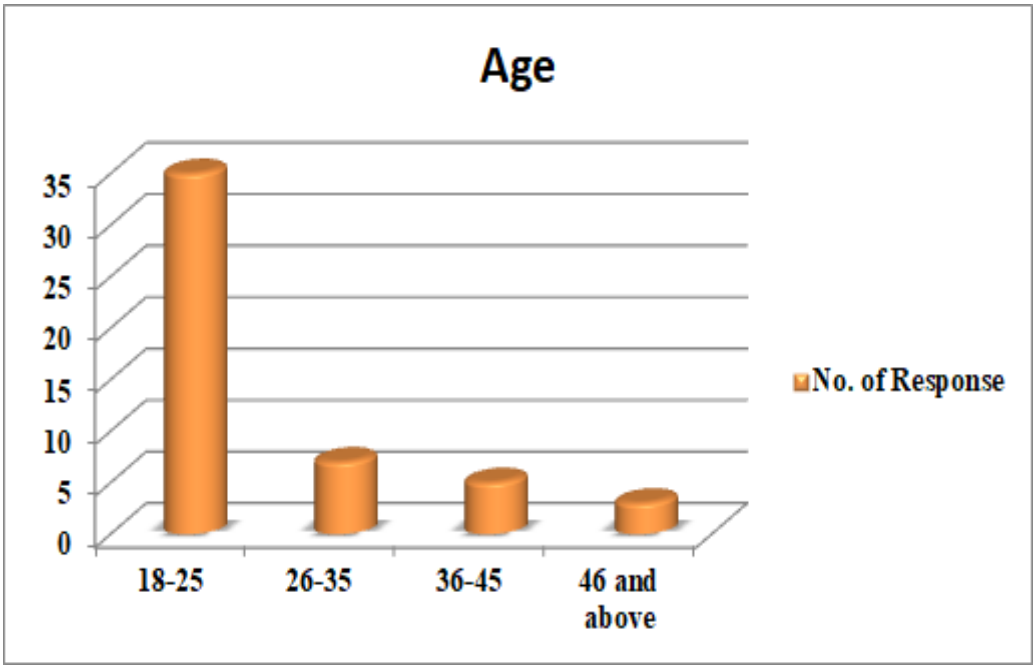

Fig. No. 4.1: Age.
Source: Primary Data.

Interpretation:

The most of respondents in this analysis (70%) are between the ages of 18 and 25 (35 out of 50). They are followed by 14% in the 26–35 age range, 10% in the 36–45 age range, and 6% in the 46+ age range. Most responders are below 36 years of age, indicating a predominantly younger population.

4.1.2. Education

The following table shows that the percentage analyses of education:

Table 4.2: Education.

Variable	No. of Response	Percentage
Bachelor's degree	26	52%
Master's degree	13	26%
Doctorate	10	20%
Other	1	2%
Total	**50**	**100%**

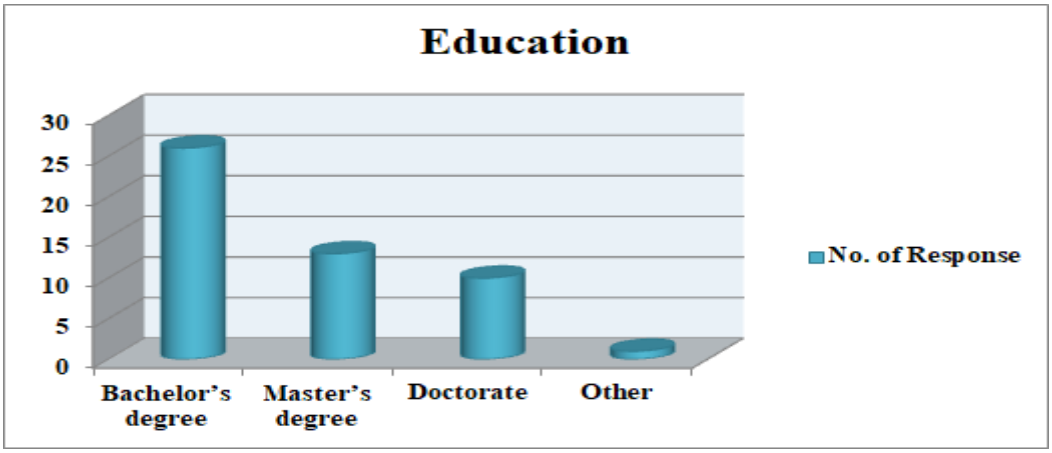

Fig. No. 4.2: Education.
Source: Primary Data.

Interpretation:

In these analyses, most of the respondents hold a Bachelor's degree, accounting for 52%, followed by 26% with a Master's degree, and 20% with a Doctorate. Only 2% reported having other qualifications. The findings show that most respondents are educated at the undergraduate level, with a notable proportion holding postgraduate and doctoral degrees.

4.1.3. Job Role In the Organization

The following table shows that the percentage analyses of job role in the organization:

Table 4.3: Job Role In the Organization.

Variable	No. of Response	Percentage
Senior Management	15	30%
Middle Management	18	36%
Information Security Specialist	11	22%
Legal /Compliance Officer	6	12%
Total	**50**	**100%**

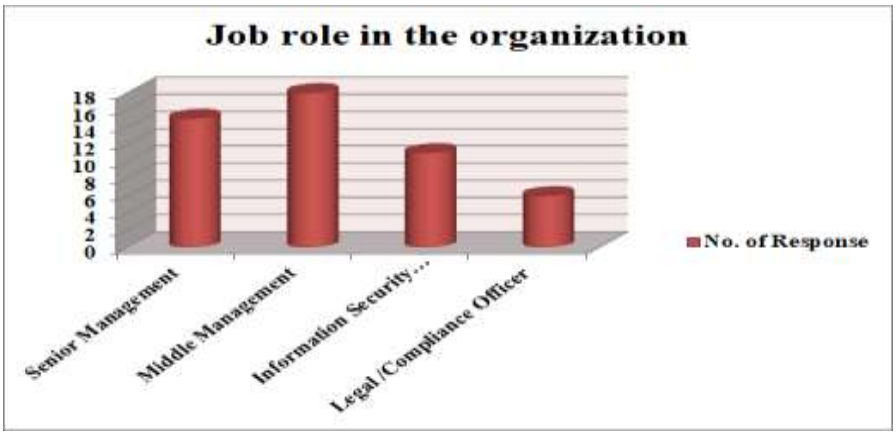

Fig. No. 4.3: Job Role In the Organization.
Source: Primary Data.

Interpretation:

In this analysis, 36% of respondents are in Middle Management, making it the largest group, followed by 30% in Senior Management, 22% as Information Security Specialists, and 12% as Legal/Compliance Officers. The results indicate that most responders are in managerial positions, with Middle Management being the most represented.

4.2. Correlation Analysis

One statistical method for determining the nature and direction of a link between many variables is correlation analysis. It makes it easier to understand how changing one variable affect changing another. The correlation coefficient, which may take values between -1 and 1, describes the outcomes of a correlation analysis. When the correlation coefficient is 1, it means that the two variables are completely related. A correlation value of -1 indicates a completely negative correlation, where the second variable decreases in proportion to the first variable increasing. With a correlation value close to zero, there is little linear relationship between the variables.

4.2. 1.Correlation Analysis Between Age and Effectiveness of Protection and Security

To test age and effectiveness of protection and security I did correlation bivariate analysis using SPSS software.

Ho: There is no connection between age and effectiveness of protection and security

H1: There is connection between age and effectiveness of protection and security

Table. No. 4.4: Correlation Analysis Between Age and Effectiveness of Protection and Security.

Descriptive Statistics

	Mean	Std. Deviation	N
age	2.00	.926	50
effectivenessofbalancingipprotectionandsecurity	3.88	1.189	50

Correlations

		age	effectivenessofbalancingipprotectionandsecurity
age	Pearson Correlation	1	.222
	Sig. (2-tailed)		.120
	N	50	50
effectivenessofbalancingipprotectionandsecurity	Pearson Correlation	.222	1
	Sig. (2-tailed)	.120	
	N	50	50

Source: Primary Data.

Interpretation:

The two variables have a correlation coefficient (r) of 0.222. This number denotes a weakly positive linear correlation. Given that the significance value (p-value) of 0.120 is greater than the 0.05 cutoff, the association is not considered statistically significant. The proposed method is unable to eliminate the null hypothesis since the p-value is higher than 0.05. This implies that the population from which the sample was taken does not have enough evidence to demonstrate a significant link between the two variables.

4.2.2. Correlation Analysis Between Education and Effectiveness of Protection and Security

To test education and effectiveness of protection and security I did correlation bivariate analysis using SPSS software.

Ho: There is no connection between education and effectiveness of protection and security

H1: There is connection between education and effectiveness of protection and security

Table. No. 4.5: Correlation Analysis Between Education and Effectiveness of Protection and Security.

Descriptive Statistics

	Mean	Std. Deviation	N
education	1.86	.881	50
effectivenessofbalancingipprotectionandsecurity	3.88	1.189	50

Correlations

		education	effectivenessofbalancingipprotectionandsecurity
education	Pearson Correlation	1	.036
	Sig. (2-tailed)		.805
	N	50	50
effectivenessofbalancingipprotectionandsecurity	Pearson Correlation	.036	1
	Sig. (2-tailed)	.805	
	N	50	50

Source: Primary Data.

Interpretation:

The two variables are correlated with one another with a value of 0.036. A practically insignificant positive linear relationship is indicated by this number. A p-value of 0.805 is far more than the 0.05 threshold, hence the connection cannot be deemed statistically significant. The recommended method cannot be used to reject the null hypothesis since the p-value is more than 0.05. This implies that the population from which the sample was taken does not have enough evidence to demonstrate a significant link between the two variables.

4.2.3. Correlation Analysis Between Job Role and Effectiveness of Protection and Security

To test job role and effectiveness of protection and security I did correlation bivariate analysis using SPSS software.

Ho: There is no connection between job role and effectiveness of protection and security

H1: There is connection between job role and effectiveness of protection and security

Table. No. 4.6: Correlation Analysis Between Job Role and Effectiveness of Protection and Security.

Descriptive Statistics

	Mean	Std. Deviation	N
jobrole	2.48	1.035	50
effectivenessofbalancingipprotectionandsecurity	3.88	1.189	50

Correlations

		jobrole	effectivenessofbalancingipprotectionandsecurity
jobrole	Pearson Correlation	1	.015
	Sig. (2-tailed)		.920
	N	50	50
effectivenessofbalancingipprotectionandsecurity	Pearson Correlation	.015	1
	Sig. (2-tailed)	.920	
	N	50	50

Source: Primary Data.

Interpretation:

The two variables have a correlation coefficient (r) of 0.015. This value indicates an extremely weak or almost no linear relationship. The correlation is not deemed significant since the p-value is 0.920, which is far more than the 0.05 level. Since the p-value is higher than 0.05, we cannot reject the null hypothesis and infer that there is no significant link between the two variables in the population from which the sample was obtained.

4.2.4. Correlation Analysis Between Experience and Effectiveness of Protection and Security

To test experience and effectiveness of protection and security I did correlation bivariate analysis using SPSS software.

Ho: There is no connection between experience and effectiveness of protection and security

H1: There is connection between experience and effectiveness of protection and security

Table. No. 4.7: Correlation Analysis Between Experience and Effectiveness of Protection and Security.

Descriptive Statistics

	Mean	Std. Deviation	N
experience	2.24	.916	50
effectivenessofbalancingipprotectionandsecurity	3.88	1.189	50

Correlations

		experience	effectivenessofbalancingipprotectionandsecurity
experience	Pearson Correlation	1	-.067
	Sig. (2-tailed)		.645
	N	50	50
effectivenessofbalancingipprotectionandsecurity	Pearson Correlation	-.067	1
	Sig. (2-tailed)	.645	
	N	50	50

Source: Primary Data.

Interpretation:

The two variables have a correlation coefficient (r) of -0.067. This number suggests a negative linear connection that is extremely weak. The relationship is not regarded as statistically significant since the p-value (significant value) of 0.645 is greater than the 0.05 limit. The recommended method cannot be used to reject the null hypothesis since the p-value is more than 0.05. This implies that the population from which the sample was taken does not have enough evidence to demonstrate a significant link between the two variables.

4.3. Regression

The multiple regression analysis shows a moderately strong correlation of 0.633 and explains 40.1 percent of the variance in the effectiveness of balancing protection and security. Whereas familiarity with pertinent policies is not significant (p-value of 0.224 and coefficient of 0.209.), the degree of effect on security is a major predictor (p-value of 0.002 and coefficient of 0.728). Interventions should focus on enhancing the extent of influence on security and improving security awareness.

Ho: There is no correlation between intellectual property awareness (including familiarity, influence, and security awareness) and effectiveness of protection and security.

H1: There is a correlation between intellectual property awareness (including familiarity, influence, and security awareness) and effectiveness of protection and security.

Table. No. 4.8: Regression Analysis Between Intellectual Property Awareness and Effectiveness of Protection and Security.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.633[a]	.401	.362	.950	.401	10.250	3	46	.000

a. Predictors: (Constant), securityawarenesslevel, ExtentofiprInfluenceonsecurity, familiaritywithippolicies

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	27.756	3	9.252	10.250	.000[b]
	Residual	41.524	46	.903		
	Total	69.280	49			

a. Dependent Variable: effectivenessofbalancingipprotectionandsecurity

b. Predictors: (Constant), securityawarenesslevel, ExtentofiprInfluenceonsecurity, familiaritywithippolicies

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.203	.679		.298	.767
	familiaritywithippolicies	.209	.169	.162	1.233	.224
	ExtentofiprInfluenceonsecurity	.728	.222	.428	3.273	.002
	securityawarenesslevel	.401	.208	.231	1.927	.060

a. Dependent Variable: effectivenessofbalancingipprotectionandsecurity

Source: Primary Data.

Interpretation:

The multiple regression analysis shows a moderately strong correlation of 0.633 and explains 40.1 percent of the variance in the effectiveness of balancing protection and security. Whereas familiarity with pertinent policies is not significant (p-value of 0.224 and coefficient of 0.209.), the degree of effect on security is a significant predictor (p-value of 0.002 and coefficient of 0.728). Interventions should focus on enhancing the extent of influence on security and improving security awareness.

5. FINDINGS, SUGGESTION AND CONCLUSION

5.1 Findings

- The majority of respondents (70%) are aged 18–25, indicating a predominantly younger population.
- Most respondents (52%) hold a Bachelor's degree, with 26% having a Master's and 20% a Doctorate, reflecting a well-educated sample.
- Regarding the job positions, 36 percent are in the Middle management, 30 percent in Senior management, 22 percent in Information security specialists and 12 percent in Legal/Compliance officers, which have a dominant managerial representation.
- The correlation analyses lead to the following conclusions: A weak positive relationship that is not statistically significant is represented by the first correlation (r=0.222, p=0.120). A very weak relationship is represented by the second correlation (r=0.036, p=0.805). A very weak relationship is represented by the third correlation (r=0.015, p=0.920). And finally, a weak negative relationship is represented by the fourth correlation (r=-.067, p=0.645).
- Multiple regression analysis indicates that the correlation between balancing protection and security is moderately strong (r = 0.633) and explains 40.1 per cent of the variance with security measures (coefficient = 0.728, p = 0.002) having significant effect and no effect of familiarity with policies (coefficient = 0.209, p = 0.224), indicating a need to increase the effect of security and awareness.

5.2. Suggestion

In order to boost the performance of any given organization and encourage its development, organizations ought to involve the young workers in custom-made programs, which appeal to the workers in their interests and needs and invest in their advanced training to exploit their high levels of education particularly in matters related to security. Management strategies and security practices can be enhanced by enhancing leadership training on managerial positions. All the employees can be sensitized on best practice in comprehensive security awareness programs, which need to focus on the need to be security conscious in their day to day tasks. Constant evaluation of correlation outcomes will be useful in determining trends and streamline strategies, especially in improving other factors of influence such as security measures. Lastly, training the appropriate policies by means of workshops and other resources will lead to an improved knowledge of the policies and adherence to them, which will eventually result in the general organizational success.

5.3. Conclusion

This paper is an empirical research study, which has explored the linkage between Intellectual Property Rights (IPR) and organizational culture in the context of information security interventions in corporate risk management systems. The results indicate that organizations that have strong IPR systems and culture of aggressiveness in their security stance are in a better position to counter any threat posed by information breach, which eventually boosts their overall security stance. Moreover, a collaborative environment with a focus on employee awareness and appeal is a strong contributor to the efficiency of defensive actions.

Finally, to overcome these challenges, which are essential to organizations to achieve the highest returns of IPR and develop a security-culture. The areas that should be re-focused in the future are the correspondence of the IPR policies and organizational values, interdepartmental interaction, and the extensive training. Through this, not only can organizations enhance their information security practices, but they can also become resilient to the new risks in the dynamically evolving digital environment.

REFERENCE S

Alhogail, A., & Mirza, A. (2021). Integrating information security into enterprise risk management: A framework for organizational resilience. *Computers & Security, 102*, 102–115.

Alnatheer, M., & Nelson, K. (2022). The role of organizational culture in proactive information security management. *Information & Computer Security, 30*(2), 234–250.

Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too close for comfort: cyber terrorism and information security across national policies and international diplomacy. Studies in conflict & terrorism, 46(12), 2426-2453.

Chang, Y., & Lin, H. (2018). The impact of organizational culture on information security management practices. *Information & Management, 55*(2), 208–218.

D'Arcy, J., Hovav, A., & Galletta, D. (2021). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 32*(1), 215–235.

Del-Real, C. (2025). A systematic literature review of security and privacy by design. International Journal of Security and Privacy, 19(1), 1–20

Herath, T., & Rao, H. R. (2019). Encouraging information security behaviors in organizations: The role of penalties, pressures, and intellectual property protection. *Decision Support Systems, 117*, 1–12.

Ifinedo, P. (2020). Critical times for organizations: What should be done to curb employees' noncompliance with information security policies? *Information Systems Management, 37*(1), 1–14.

Kshetri, N. (2018). Cybersecurity and intellectual property protection in emerging economies. *Journal of International Management, 24*(3), 1–15.

Lu, W., & Wu, L. (2024). A blockchain-based deployment framework for protecting building design intellectual property rights in collaborative digital environments. Computers in Industry, 159, 104098.

Oruc, A., Chowdhury, N., & Gkioulos, V. (2024). A modular cyber security training programme for the maritime domain. International Journal of Information Security, 23(2), 1477-1512.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124, 102974.

Shaikh, F. A., & Siponen, M. (2023). Internal organizational factors in information security management: The role of culture, leadership, and employee awareness. Information & Management, 60(2), 103–118.

Straub, D. W., & Welke, R. J. (2019). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 43(3), 987–1010.

Von Solms, S., & Von Solms, R. (2020). Information security governance: A model based on corporate governance principles. *Computers & Security, 92*, 101–118.

Wang, F., Gai, Y., & Zhang, H. (2024). Blockchain user digital identity big data and information security process protection based on network trust. Journal of King Saud University-Computer and Information Sciences, 36(4), 102031.