Sci. Educ. Innov. Context Mod. Probl. P-ISSN: 2790-0169 E-ISSN: 2790-0177
Issue 1, Vol. 8, 2025, IMCRA

A Statistical Research: The Effectiveness of Information Security Culture in Organizations concerning Organizational Culture

K. Sarvani

ORCID: 0000-0002-3160-4574
Symbiosis Centre for Information Technology, Symbiosis International (Deemed University),
Pune, India, k_sarvani@siu.edu.in

Vidyavati Ramteke

ORCID: 0000-0002-6483-7438
Symbiosis Centre for Information Technology, Symbiosis International (Deemed University),
Pune, India, Email Id: vidyavati@scit.edu

Received date: 10.01.2025; Accepted date: 16.03.2025; Publication date: 24.04.2025
doi: 10.56334/sei/8.1.83

Abstract

Information is now the most important asset that a person, an organization, or business needs, and securing it will always be on headlines. Researchers say that "Information Security (IS) is not an IT problem anymore; it is a business issue." Maintaining information security is becoming more challenging day by day as the involvement of humans prevails in both causing damage to information and protecting it. As human is the weakest link in securing information, there is a need to look into the relationship between organizational culture (OC) and Information Security Culture (ISC) in an organization. Researchers have found the relation between the behavioral aspects of an employee and ISC. This paper shows a statistical relation between the four types of OC and ISC and a framework which shows the ranking among the culture types, is also depicts the importance given by each culture to Information Security considering confidentiality, availability, and integrity of information. The four types of OC (Clan Culture, Hierarchy Culture, Adhocracy Culture, and

Citation. K. Sarvani, Vidyavati R. (2025). A Statistical Research: The Effectiveness of Information Security Culture in Organizations concerning Organizational Culture. *Science, Education and Innovations in the Context of Modern Problems*, 8(1), 1252-1265. doi: 10.56352/sei/8.1.81. https://imcra-az.org/archive/356-science-education-and-innovations-in-the-context-of-modern-problems-issue-1-volviii-2025.html

Market Culture) as per Competing Value Framework were mapped against IS triad with ranking given to the OC. From the analysis done, the research outcome was that Hierarchy Culture gives utmost importance to ISC, thus giving the organizations a set of qualities that can be imbibed.

Keywords: Organizational culture, Information Security, Information, Behavior, Information Security Culture, Safety.

1. Introduction

Today's business world functions with a huge amount of information used for internal and external decision-making in any organization. Information is a non-tangible asset to organizations, the need to secure it becomes a necessity as human vulnerabilities and threats are increasing day by day [1]. Information security is a practice of safeguarding data confidentiality, maintaining data integrity, and ensuring data Availability [2]. Securing information enables smooth functioning of an organization, protects from disruption of day-to-day processes and inculcates trust towards collected information in any organization [3].

Organization Culture includes the vision, mission, norms, systems, beliefs, and habits of an organization. While information security may be a major concern any organization is facing, introducing security measures and practices in their culture could affect the organization's success in a positive way [4]. With this, introduce the competing value framework (CVF), which is a tool used by most organizations to map their culture with one of the types of OC. It is the most dominant and widely used model within the area of OC research [5].

It has been approved as one of the 40 most influential models in business history. It has been used in quite several organizations to foretell the performance of the organization. Based on the research on CVF, each type is summarized as below and shown in Figure 1.

1.1. Type 1 - Clan Culture: Organizations with Clan culture are like a family with a lot in common with an atmosphere of collectiveness and helping nature among employees [6]. These firms emphasize giving authority when required, teamwork, and employee progress.

1.2. Type 2 – Adhocracy Culture: In these organizations, the employees are always willing to take chances, and leaders are seen as innovators willing to take risks [7]. This culture arises within any firm when there are new tasks where risk-taking becomes mandatory to compete and ends when not required. Hence, its name is 'Ad-hoc'.

1.3. Type 3 – Market Culture: The goal of these organizations is to get business, get work done and achieve results with a competitive nature among employees [8]. The focus is to capture market share to the maximum and gain huge profits focusing on the external business environment.

1.4. Type 4 – Hierarchy Culture: These organizations have strict rules and regulations set by top management and to be followed by all the employees. It has a clear structure of organization, systematic procedures, strict control, and circumscribed responsibilities. Leaders will continuously monitor and mentor

the employees for desired results.

It is believed that an organization's corporate culture has a huge influence on information security. OC defines an employees' perspective towards the organization. It is observable that it is evolving and changing as time passes, and it can either be created by the top management or by the employees themselves [9]. As the cyber threats are growing drastically, there is a need to understand how organizational culture impacts information security practices in an organization [10]. Hence, the primary objective of this paper is to find the impact of different organizational cultures on the effectiveness of IS.

By the definitions of ISC and OC, an inference can be drawn that there can be a relation between them [11]. Although many researchers have concluded that there will always be an impact of OC on ISC, given the relation between them and built various models, the variables and parameters chosen from OC were more into personal behavior of employees in a firm [12]. Many types of research are done on the types of organizational culture formed from the Competing Value Framework [13]. This paper fills the gap of determining a relationship between the types of OC and ISC.

The purpose of this paper is to determine the impact of types of OCs on ISC to know which type among them can effectively secure sensitive information and list down the qualities an organization needs to teach to adhere to the information security policies, practices, and standards [14]. This research answers the following underlying Research Questions (RQ): RQ1: Which type of organizational culture effectively handles securing their information? RQ2: What set of qualities an organization needs to teach to secure their sensitive information?

The entire paper further is divided into sections which include a review of literature, methodology of the study, the research framework, an analysis of the relationship between each type of organizational culture with the effectiveness of information security culture in results and discussion, the conclusion of the study, the scope for future research and research limitations [15].

2. Literature Review

2.1 Role of Information Security in An Organization

The amount of data generated and processed per hour, a minute or second indicates the 'Volume of data, the speed at which this data is generated refers to 'Velocity,' the various forms of data is its 'Variety,' the quality and accuracy of data is its 'Veracity' and Value created for this data resides in organizational capability of turning this data into meaningful business insights.

With the continuous evolution of the Internet, the number of electronic transactions among organizations has increased with the volume of data or information. The need for securing this information rose drastically.

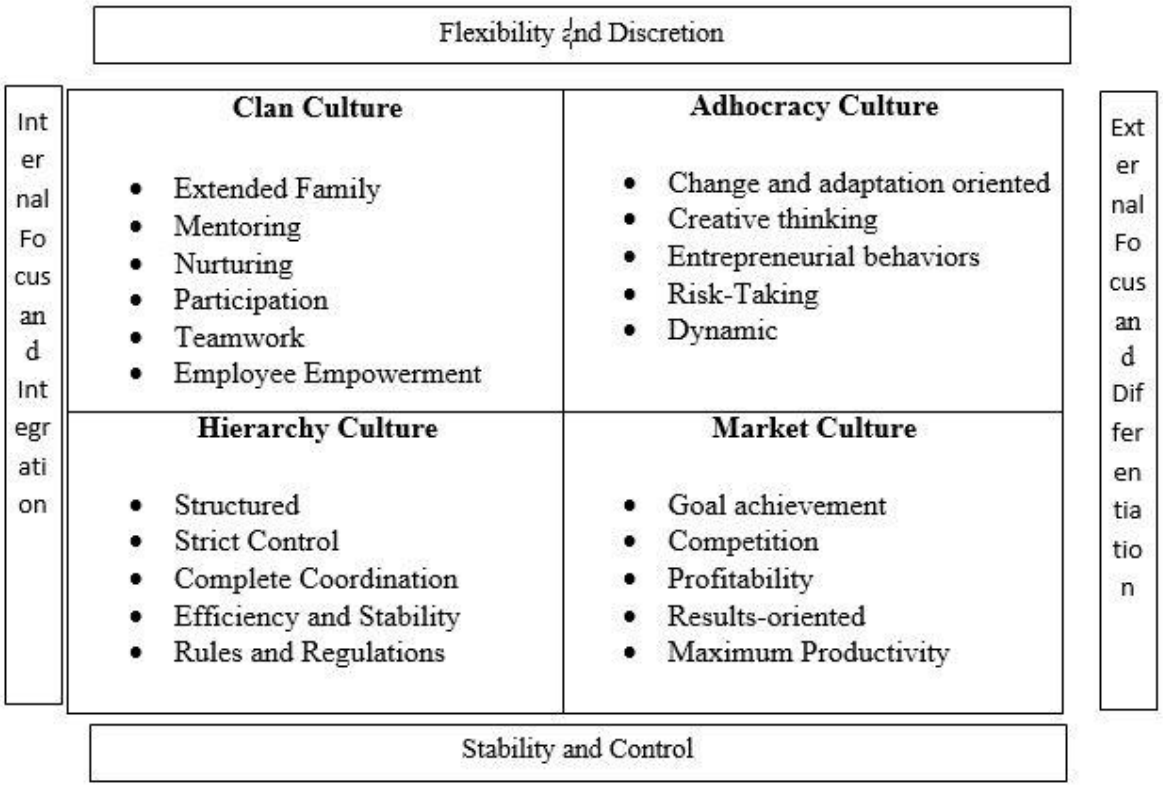

Figure 1. Types of Organizational Culture. Source: (Quinn & Cameron, 1988).

T is defined as the process followed to shield the information from exposure to many threats to ensure continuity of business activities, reduce the damage caused to business and maximize return on investment. Hence, IS plays a crucial role in planning and company management. The main objective of securing information is to ensure the principles are rightly followed, popularly known as the CIA triad. Confidentiality (C) is a property where information is disclosed only to authorized people, integrity (I) is to ensure the exactness of information, and Availability (A) is to provide access to that information, to which right people are bound to access and at the right time. The current research sees a different aspect where the point of concentration is organizational IS. The values and beliefs prevailing in the organization within its cultures influence the CIA of data. Thus, managing information security becomes essential. Information security management is a concept that makes sure a necessary level of security is maintained with obtained and processed information. Research done worldwide on information security shows that the maximum attacks caused were malware and phishing by the employees, former employees, suppliers, and contractors. The types of organizational culture are shown in Figure 1.

3. Organization Culture

Organizational culture refers to a set of values, standards, and perspectives of a bunch of people that reflects the behavior of the employees. In today's business world, humans are considered the main capital of organizations, and employees are the basic unit of work, yield, and progress of an organization. The aspects of organizational culture are values – way of functioning and interpersonal relations, standards, and patterns of behavior in various situations. The behavior of a person depends on the way he perceives a situation. OC has been conceptualized by values that differentiate one organization from other. This research has considered a huge set of characteristics.

OC is formed by various factors, which include the existence or non-existence of truth and rationality in the organization, the concept of planning, goal setting, or focus of the employees, motivation and personal growth, commitment towards work, isolation versus cooperativeness among the employees and by the behaviors of dominant organization members like top management.

Literature talks about two frameworks of OC, namely National Culture Framework and Competing Value Framework (CVF). The segregation of an organization's behaviors based on individual maintenance, flexibility, external positioning, and gradual change. CVF is a precious tool to show the underlying surface model and also overlying regular activities of the organization. It was developed to look at how effective an organization is. It is an instrument to indicate the synergies that may subsist or can be introduced in the organization for operating in a better manner. Based on initial research on CVF, researchers have identified indicators of organizational effectiveness, which usually reflect personal values from which three value dimensions were derived. The three dimensions were internal-external, control-flexibility, and means-ends. An argument arose that these three dimensions were not sufficient to decide on the OC values. The research is done to answer the argument led to the evolvement of a model with a set of values under each type shown in Figure 1. The culture of organizations revolves around factors like employee participation in decision making, teamwork adaptation to change, creative thinking, inclination towards goal achievement, internal efficiency, rate of successes and importance given to rules and regulations. However, CVF assumes that all the types of OC can exist in an organization as a mixture simultaneously. In any given organization, one of the types can dominate over others; in others, all the types will combine to form a balanced culture. With this, OC can be defined as "The way an organization behaves in a specific situation." A detailed definition states that "A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well to be considered valid and therefore, to be taught

to new members as the correct way to perceive, think and feel in relation to those problems.". SC is part of corporate culture and defines how employees see the organization. Literature highlights that OC is a system of learner behavior that is reflected in the end-user awareness and behavior in information security.

3.1. Information Security Culture

ISC, in a holistic view, becomes a part of organizational culture, including people, process, technology, and communication. With the rise of mobility and Bring Your Own Device (BYOD), organizations require guidance in implementing an appropriate stringent ISC. IS is the property of making an organization's valuable information undisclosed to unauthorized persons available to authorized persons and simultaneously ensuring its accuracy. While safeguarding the information, organizations have the need to mitigate the threats from various sources. Hence, managing IS is based on controlling the received, processed and residing information. Recent studies have shown that the establishment of an organizational ISC is essential for effective IS. However, OC might have a significant influence on the IS, and this could be positive or negative.

A corporate ISC must abide by the policies, methods, responsibilities, and procedures of a company in a way where it becomes a part of the daily activities of an employee. The split of ISC can be the value given to information security characteristics by an organization, an employee having the power of distinguishing between acceptable and unacceptable actions in regard to information security and differentiating between the behavior which is encouraging and which is not. With this, an employee will turn into a valuable security asset. Managing ISC plays a crucial role in the process of securing information. It is a cycle of multiple and frequent evaluations, change, and maintenance. Researchers have pointed out that ISC is an important factor in maintaining a respectable and satisfactory security level in organizations and have declared that only a required amount of change in security culture can minimalize the number of security threats following the CIA triad of IS. The literature presented a conceptual framework that describes the composition of new entities based on interactions of entities at different levels. It will assist in establishing the role that is played by ISC in the management of IS in organizations.

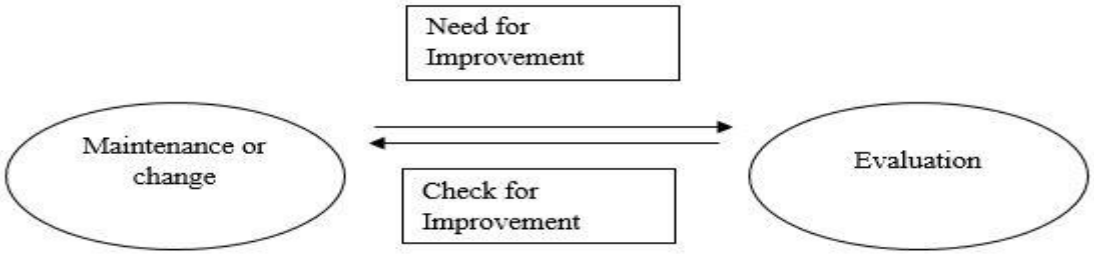

Figure 2. The ISC Management Cycle. Source.

The first step is to analyze the current situation in the organization, identify loopholes in the system, and check for improvements to be made in the culture if it does not fit the ISC standards. This process cycle is indicated in Figure 2.

In today's world, the reality shows that research on information security cannot rely only on technical aspects as there is always room for constant changes in this field. This raises the need to look into the aspects other than technical issues, which are social and organizational ones. It also pertains to be a major worry among the top management at the highest level of organizations in safeguarding their information.

3.2. Relation between OC and ISC:

Each organization is unique and develops a culture under the influence of multiple factors; national culture may also be one of them. Literature also talks about the national culture influencing organizational security culture, which is part of OC, influence human behavior. Three types of relations can be interpreted from the literature listed as 1. ISC is separated from OC, where the organizations do not follow the practice of securing information at all, and 2. ISC, as a part of OC, members within the department are trained for security maintenance with a lack of inter-departmental coordination in following security policies and 3. ISC is embedded into OC, where the responsibility of information security lies in the blood of the organization. However, this can be related to a similar study on human behavior towards following the information security practices. According to this study, the preparedness and responsibility of the employees, management support, and strictly following the regulations lead to the enhancement of information security. An organization's information security policy should convey a plan of action (i.e., its purpose, goals, importance, and activities) and document who is responsible for security-related agenda across the organization. A number of organizations are moving to the cloud, increasing the risk of cyber-attacks. The three elements for organizational transformation are People, Process, and Technology, where people from the ultimate cause for cyber-attacks making true the saying, "People are the weakest link in cyber security".

The reason behind this is their security behavior when handling information assets. A causal relationship was discussed among the OC divided as Loose vs. Tight Control, Process vs. results-oriented, Employee vs. Job Oriented, and Open vs. Closed System, Normative vs. Pragmatic OC on Compliance, Accountability, Governance, and Communication of the organization. Literature shows a huge impact of OC on ISC. Various aspects of OC in relation to ISC were covered in the past researches leaving a gap to carry out research on the dependency of types of OC on ISC.

4. Methodology

The study aimed at collecting responses of employees from various organizations to assess their opinions on their organizational culture and the importance is given by their organization to information security culture.

Specific attention was given to the types of organization cultures mentioned above with the respective qualities under each. The aim of the paper is to draw a relation between OC and attributes of ISC and rank them based on the effectiveness of ISC in each organization type. The stepwise approach of the study is as follows:

4.1. Data gathering

To develop a framework that shows the dependency of OC on ISC in organizations, the assessment tool is a questionnaire that is used to collect responses from employees of different organizations. Different variables like mentoring, employee participation, and teamwork under each OC type and in information security like confidentiality, integrity, and availability were considered to draw a relation after analysis of the data collected. The reason for collecting data from various employees of different organizations is to get the hang of the culture of different organizations.

4.2. Questionnaire Development

The questionnaire is divided into three sections; the first section is personal information. The second section contains questions related to the culture of the organization, which includes one question each for parameters like organization feel like an extended family for the employees, mentoring, effective communication, employee participation, teamwork, employee empowerment, risk-taking, adoption of change, dynamic, strict control over employees, goal achievement, maximize productivity and results-oriented organization.

The third section includes questions to assess the importance given by each of the organizations to

information security culture considering the parameters like confidentiality, integrity, and availability of data in respective organizations.

Statements have been framed in such a way that they represent each quality of organizational culture and the information security triad. Responses are collected in a 5-point Likert scale format from the employees, which shows the extent to which an employee agrees or disagrees with a statement. The responses received were close to 200, which is the sample size considered for the study. The items mentioned in the questionnaire give information about both OC and the importance given to security, which is further helpful in drawing a relation between them. Items in the questionnaire are shown in Table 1.

Table 1. Items in the Questionnaire.

Variable	Sub variable	Qualities/Indicators	Number of Items
Organizational Culture	Clan Culture	Communication, mentoring, employee participation, teamwork.	6
	Adhocracy Culture	Change adoption, risk-taking, dynamic in nature	3
	Hierarchy Culture	Rule and regulations, strict control over employees, efficiency	6
	Market Culture	Results-oriented, maximize productivity, goal-oriented	4
Information Security Culture	Confidentiality	Secrecy, Access right, backup	3
	Integrity	Completeness of information	1
	Availability	Availability of information at the right time	2
Total items in the questionnaire			25

5. Results and Discussion

This research framework shows the relationship between the type organization cultures and the information security triad. It also shows the ranking of each type of culture in terms of the importance given to the information security triad of the respective OC. However, this study only captures the importance given by the organizations to three aspects of IS that is the CIA triad of information. As part of data analysis, this paper aimed to test four hypotheses which are:

H1: Organizations with Clan Culture give importance to Information Security Culture.

H2: Organizations with Adhocracy Culture give importance to Information Security Culture.

H3: Organizations with Hierarchy Culture give importance to Information Security Culture.

H4: Organizations with Market Culture give importance to Information Security Culture.

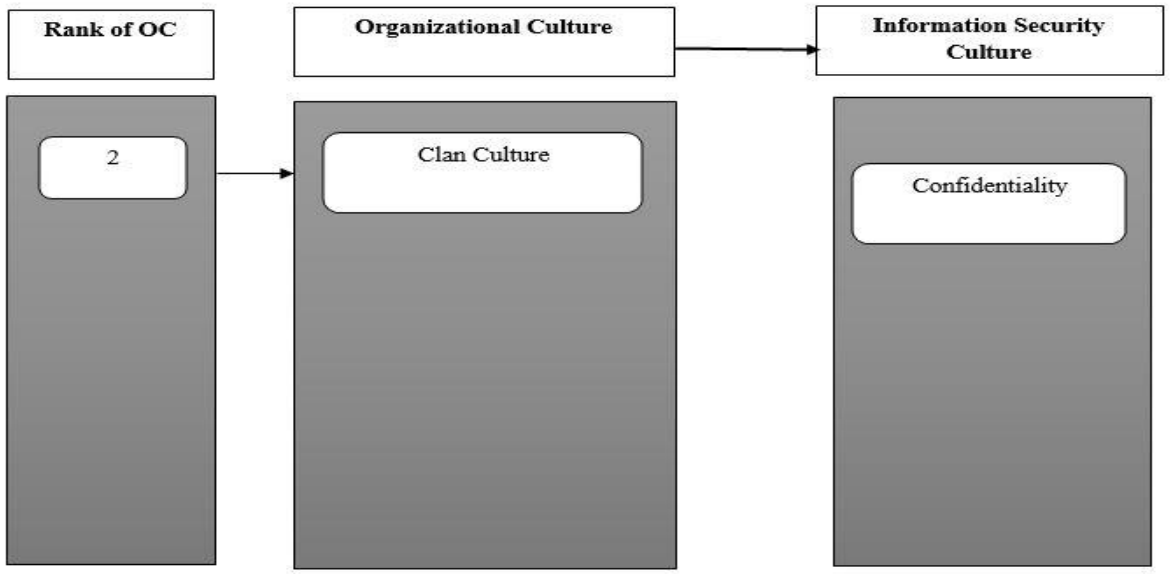

Figure 3. The Research Framework.

Figure 3 shows the research framework. All the responses were collected, and sub-variables of each type of organizational culture were segregated and grouped under one type of culture. Similarly, the responses related to the information security triad were also segregated for analysis.

From the available data of OC, six sub-variables were grouped under Clan culture, three sub-variables grouped under Adhocracy culture, six sub-variables grouped into hierarchy culture, and four under the market culture. In each type of culture, the mean of all the sub-variables was calculated for each response. For instance, for clan culture, the mean of all the six sub-variables for each response was calculated.

For information security culture, the responses for all three aspects were recorded, and the mean of

each response was calculated.

Considering both the means of OC and ISC for each type of OC, a two-sample t-test for means was calculated, resulting in organization culture score and information security culture score.

5.1. Hypothesis 1: Organizations with Clan Culture Give Importance to Information Security Culture.

After applying the t-test assuming variable one as means of clan OC sub-variables and variable two as means of ISC aspects, resulted in p-value=0.31, which is greater than 0.05(significance level), shows that the organizations with clan culture give importance to ISC (as both the means are equal and null hypothesis is accepted) which in turn proves that they follow ISC effectively.

As the p-value indicates the probability of the null hypothesis being true, from the observed data analysis, it is concluded that the probability of organizations with clan culture giving importance to ISC is 31% taking second place among all.

5.2. Hypothesis 2: Organizations with An Adhocracy Culture Give Importance to Information Security Culture.

After applying the t-test assuming variable one as means of Adhocracy OC sub-variables and variable two as means of ISC sub-variables, resulted in p-value=0.02, which is less than 0.05(significance level) shows that the organizations with Adhocracy culture give less importance to ISC (as both the means are unequal and null hypothesis is rejected) which in turn proves that they do not follow ISC effectively.

As the p-value indicates the probability of the null hypothesis being true, from the observed data analysis, it is concluded that the probability of organizations with adhocracy culture giving importance to ISC is 2% taking third place.

5.3. Hypothesis 3: Organizations with A Hierarchy Culture Give Importance to Information Security Culture.

After applying the t-test assuming variable one as means of Hierarchy OC sub-variables and variable two as means of ISC aspects, resulted in p-value=0.49, which is greater than 0.05(significance level), shows that the organizations with hierarchical culture give importance to ISC (as both the means are equal and null hypothesis is accepted) which in turn proves that they follow ISC effectively.

As the p-value indicates the probability of the null hypothesis being true, from the observed data analysis, it is concluded that the probability of organizations with clan culture giving importance to ISC is 49% taking the first place, which is the topmost.

5.4. Hypothesis 4: Organizations with Market Culture Give Importance to Information Security Culture.

After applying the t-test assuming variable one as means of Market OC sub-variables and variable two

as means of ISC aspects, resulted in p-value=0.06, which is far less than 0.05(significance level), shows that the organizations with market culture give quite less importance to ISC (as both the means are unequal and null hypothesis is rejected) which proves that they do not follow ISC effectively.

As the p-value indicates the probability of the null hypothesis being true, from the observed data analysis, it is concluded that the probability of organizations with adhocracy culture giving importance to ISC is 6% taking the last place.

Based on the above results, each type of organizational culture was ranked against the effectiveness of information security culture, as shown in figure 3. The advantage of this analysis and research framework is, organizations get to know that there is an impact of OC on information security which is the prime necessity of any firm these days, and what are the qualities to be imbibed in the organizations? to secure their information.

6. Conclusion

There are a large number of organizations with different levels of priority given to IS within the organization. The outcome of this paper shows that there is a dependency of types of OC mentioned above on ISC. This research helps the new entrants pick qualities to be imbibed in their organizations based on their priority towards securing information, and existing organizations can work towards changing their approach in securing information as required. This paper successfully answers the research questions mentioned in the above sections; that is, the organizations with hierarchical culture give utmost importance to information security culture and so its qualities.

For further research, a study can be conducted on various other aspects of information security like Accountability, Identification, Authentication, Authorization, and Non-Repudiation. The limitations of this research are, being known that the culture of organizations is different in each country; it does not consider the difference of OC in different countries. It does not include other principles of information security which are also important aspects to be considered while researching.

References

Akhyari, N., Ruzaini, A.A. and Rashid, A.H., 2018. Information security culture guidelines to improve employee's security behavior: a review of empirical studies. Journal of Fundamental and Applied Sciences, 10(2S), pp.258-283.

Alhassan, M.M. and Adjei-Quaye, A., 2017. Information Security in an Organization. International Journal of Computer (IJC), 24(1), pp.100-116.

AlHogail, A., & Mirza, A, 2015. Organizational Information Security Culture Assessment. Int'l Conf. Security and Management | SAM'15 |, pp. 286-292.

Another, Mohammed A., 2014 "A conceptual model for understanding information security culture."

International Journal of Social Science and Humanity, 4(2), pp. 104.

Alnatheer, M. and Nelson, K., 2009. Proposed framework for understanding information security culture and practices in the Saudi context.

Chmura, J., 2016. The impact of positive organisational culture values on information security management in the company.

Connolly, L.Y., Lang, M., Gathegi, J. and Tygar, J.D., 2016. The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study. In HAISA (pp. 33-44).

Giritli, H., Oney-Yazici, E., Topcu-Oraz, G. and Acar, E., 2006. Organizational culture. A comparative analysis from the turkish construction industry CCIM2006 Sustainable Development through Culture and Innovation, pp.26-29.

Greene, G. and D'Arcy, J., 2010, June. Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In 5th Annual Symposium on Information Assurance (pp. 1-8).

Hartnell, C.A., Ou, A.Y. and Kinicki, A., 2011. Organizational culture and organizational effectiveness: a meta-analytic investigation of the competing values framework's theoretical suppositions. Journal of applied psychology, 96(4), p.677.

Hassan, N.H. and Ismail, Z., 2012. A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia-Social and Behavioral Sciences, 65, pp.1007-1012.

Hassan, N. H., Ismail, Z., & Maroon, 2015. N. INFORMATION SECURITY CULTURE: A SYSTEMATIC LITERATURE REVIEW. Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015, pp. 456-463.

Helfrich, C.D., Li, Y.F., Mohr, D.C., Meterko, M. and Sales, A.E., 2007. Assessing an organizational culture instrument based on the Competing Values Framework: Exploratory and confirmatory factor analyses. Implementation science, 2(1), pp.1-14.

Kokt, D. and Van der Merwe, C.A., 2009. Using the competing values framework (CVF) to investigate organisational culture in a major private security company. South African Journal of Economic and Management Sciences, 12(3), pp.343-352.

Kumarapandian, Shamganth, 2018. "Melanoma classification using multiwavelet transform and support vector machine." International Journal of MC Square Scientific Research, 10(3), pp. 01-07.