The Effective Leadership Style in Health Sector of Pakistan and Its Impact on Information Security

AJAB KHAN BURKI
Department of Management Sciences, Bahria University Islamabad, Pakistan.

Abstract

Purpose – The purpose of this paper is to examine the most prevalent Leadership style in health sector (i.e. Hospitals) of Pakistan and to explore the impact of leadership on Information security and their mutual relationship. **Design/methodology/approach** – This paper's approach is quantitative and involved data collected from 107 respondents of 73 hospitals through a questionnaire. The respondents were administrators or doctors or both at the same time from various private and public hospitals. The questionnaire comprised 5 questions for 'Leadership concern for Production', 7 questions for 'Leadership concern for people' and 7 questions for 'Information security'. For effective analysis the results, the data have been obtained through the following cities of Pakistan, namely; Karachi, Lahore, Islamabad, Peshawar, Hyderabad, Larkana, Khairpur, Sukkar, Dera Ismail Khan, Bannu, Sarai Naurang, Karak and Tank. For analysis and accurate output SPSS and MS Excel are used..**Findings** – The analysis revealed that Team Management/Leadership is the most predominant style in health sector (i.e. hospitals) of Pakistan. Majority of the respondents replied that the aforementioned style has greater correlation with the information security practices. This study is beneficial for all those individuals who really want to have a deep insight into the exploration of leadership style and its impact on information security practices within Health sector (i.e. hospitals) of Pakistan.**Research limitations/implications** –This study does not show individually and independently the leadership style and its impact on information security of private as well as public hospitals.**Originality/value** – This study is one of the first studies to empirically demonstrate the most prevalent leadership style in health sector (i.e. hospitals) across Pakistan and to determine its impact on information security practices.

Keywords: information security, leadership, privacy, confidentiality, People, Task

1. INTRODUCTION

Leadership is defined as a "social influence process in which the leader seeks the voluntary participation of subordinates in an effort to reach organizational goals" (Robert Kreitner, Angelo Kinicki, 2004).

There are various views about leadership but generally it can be classified into 12 categories (Bass, 1990).

1. the focus of group processes;
2. a matter of personality;
3. a matter of inducing compliance;
4. the exercise of influence;
5. limited to discretionary influence;
6. an act or behavior;
7. a form of persuasion;
8. a power relationship;
9. an instrument of goal performance;
10. an emerging effect of interaction;
11. the initiation of structure; and
12. a combination of elements

The effective leadership should have the following qualities: clarity of vision; excellent communication and interpersonal skills, honesty, openhandedness, self-mastery and a strong level of motivational and physical energy (Tait, 1996). Leaders are mainly responsible for setting the codes of the organization and this is reflected that how tasks are approached, how the organizational guidelines are interpreted and more specifically how employees are treated (Taylor and Taylor 1996).

1.1 The various leadership styles and its consequences:

There are various styles of leadership that influence the followers in different ways according to its use with respect to culture.One study argues that leadership style affects the group work processes, social climate and finally the outcomes. In other words when social climate is affected, it directly affects the productivity and creativity. (G.Evkall, et al., 1997).Old studies shows considerable positive correlation between corporate culture and effective leadership style for the enhancement of organizational commitment and to increase the consistency of employee behaviour. (Ogbonna and Harris, 2000; Lok and Crawford, 2004).

Leadership style not only affects the final results but it also has a great relation with numerous other factors, like it has immense affects on various variables like flexibility, responsibility, standards, rewards, clarity and commitment. In some cases it has its implications for organizational climate. (D. Goleman, 2000).Similarly the main aspect of organization, performance-- which is related to innovative and competitive culture is too affected by the leadership style. (E. Ogbonna, 2000).The decision of an organization is related to the performance evaluation of the employees.The leadership style with regard to decision analyze various factors such as the relevance of decision, the significance of commitment, the probability of success, the expertise of the leader and its team's support for achieving the desired goals. (V. Vroom,2000). It is mandatory that the employees should be taken into confidence prior to take any effective decisions regarding the organizational objectives. Managers should appreciate heterogeneity of ideas and values in the organization for effective decisions to be made (Alvesson,M., 2001). The successful leaders always keep a flexible approach to solve any issue.Hence the successful and The Strategic Leadership means the capacity to learn, the capacity to change, and knowledge of the organization (Boal,K.B, hooijberg,R,2001). Mumford (1994) examines the various leaders for their approaches to learn and accommodate accordingly.

There are four approaches which are the basic sources for leaders to improve work as well as learn from them.

- ***The intuitive approach:*** learning from past experience. So the better managing and organizing can be achieved once a leader is confronted with new challenging circumstances.
- ***The incidental approach:*** it's learning by chance from activities that inculcate within individual the true spirit to anticipate and tackle the issues.
- ***The retrospective approach :*** this include learning and improving by reviewing all the past mistakes and to draw a safety line for future.
- ***The prospective approach :*** this is the fore step approach in which retrospective components and elements of planning are included for tasks. Leader here turn to learn from variety of experiences.

1.2 The more predominant leadership styles by Blake and Mouton:

It can be better understand by understanding the Leadership Grid developed by R. Blake and Adams McCanse.

Managerial Grid (Blake and Mouton, 1964)

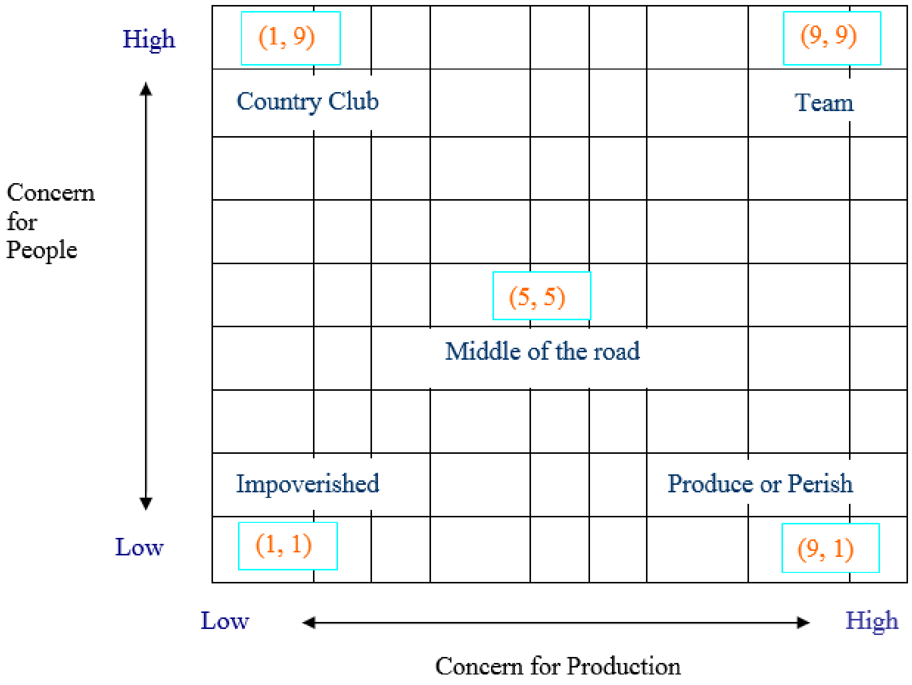


Figure: 1. the leadership Grid or Management Grid By Blake and Mouton

The leadership Grid or managerial grid is developed by two famous doctors, Robert R. Blake and S. Mouton (Grid International, Inc.).The above model of Blake and Mouton are self-explanatory and describes attitudes, Behaviors and way of thinking of various leaders in terms of their vital concern for the mentioned cross-sectional outcomes from Horizontal i.e. concern for production and Vertical i.e. concern for people scenarios. The Managerial Grid is based on two behavioral dimensions (Mind Tools Ltd, 1995-009):

- **1.2.1.Concern for People** – the leader takes care for the needs of team members, their interests, growth and development while deciding how better to achieve task.

- **1.2.2.Concern for Production** - The leader emphasizes mainly on objectives, organizational efficiency and high productivity when taking any decision about the tasks to be accomplished.

The above all styles are termed to be happened in one shape or the other depending upon the attitude and behavior of the leader and mainly upon the culture of that organization. Some leaders have great concern for production only. Some of the illustrations of the grid are discussed as below;

Impoverished Leadership- low production/low people **(1.1):**

This type of leadership is neither have a high regard for the creating the systems for getting the task done by the employees, nor creating atmosphere that is motivating and satisfying. The leader of such caliber is responsible for disorganization, dissatisfaction and disharmony among the employees. It is often referred to as Laissez-faire leadership.

Authority Compliance Management or Produce or Perish Leadership - High Production/Low People **(9.1)**:

This type of leadership approach is autocratic in nature. The employees are considered secondary to tasks of the organization i.e. such leaders believe employees only mean to an end. This type of leader has very strict working rules, policies and procedures. They consider punishment as the effective tool for the motivation of employees and to get the work done through them.

Middle-of-the-Road Leadership - Medium Production/Medium People **(5.5)**:

This leadership approach seems to be a balance of two competing concerns. In this style the leader tend to remain in the mid of two extremes by taking care of both the people as well as task. The leadership mindset here is to compromise each concern so that neither the production nor the people needs may be fully negated. Such leaders are average performers. It's believed that pragmatically this style is of greater importance.

Country Club Leadership - High People/Low Production **(1.9):**

This type of leadership is mainly concerned for the needs and feelings of the team members. These people are under the assumption that as long the team members are happy and secure, they will put their hearts and soul for the achievement of organizational objectives. The work atmosphere is very relaxed and fun. Here the production suffers due to lack of direction and proper control.

Team Leadership - High Production/High People **(9.9):**

This is the most efficient leadership style. These leaders care both for production as well as needs of the people on equal footings. Here the employees believe a stake in the organization's success. Such feelings are inculcated in them by the leaders that in return create an atmosphere of trust and respect among all the ranks and files of the organization. This approach leads an employee towards high satisfaction and motivation and, as a result, high production. According to Jeffrey Gandz , Leadership is all about achieving the objectives of the organization. If a leader achieved it then the followers will support him/her but as against if a leader does not come up to the desired expectation of the employees or accomplishing goals then the subordinates will not support in spite of either charismatic attributes or any other style of leadership.(Jeffrey Gandz, 2005).According to Blake and Mouton, the most liked style of leadership is the 'Team Management' where maximum productions along with the optimal satisfaction of the people are attained. While the most lethargic leadership style is 'Impoverished Style' where disharmony, dissatisfaction and disorganization of employees remain there in place due to less interest by the leader in tackling the organization with the set objectives and goals.(what is managerial grid model, access 2008).

There are several styles of leadership such as: autocratic, bureaucratic, laissez-faire, charismatic, democratic, participative, situational, transactional, and transformational leadership (Mosadeghrad 2003b, 2004).There is no common consensus as to which of the above mentioned style is the most appropriate. It depends upon the situation as no one leadership style is ideal for every situations. Transformational leaders are characterized by the ability to bring about change, innovation and entrepreneurship" (Ulukan, 2005).

1.3. The impact of leadership styles on Information security:

Information security is defined by various authors according to their own perceptions and ideas behind their given definitions. Information security includes technology, people and processes. Some of the technical measures such as passwords, firewalls and biometrics are used to stave off threats to information. For this, many organizations adopt different measures to incorporate and ensure the reliability of security for the information, just like training, specifying policies, rules and regulations for it Some of the authentic definitions are given below;Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.(Cornell law school,2008).Security of information is a roader term which encompasses the protection of privacy and confidentiality and also to keep integrity and accuracy. Its generally processes both technical as well as organizational for the security and protection of information collection, storage and transmission. (Beauchamp & Childress, 1994).According to surveys by Research Concepts LLC (202), security is the sole critical factor of IT professional in relation to e-business. The most common goals in information security to achieve are confidentiality, integrity and availability of information. Another definition according to business dictionary is," Safe-guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity." Information security is one of most vital issues confronting organizations across the globe. As the modern businesses and economies are totally dependent on Information technology for effective growth and survival, the need to protect information is now more prominent than ever earlier (President, 2003).Many national surveys indicate a greater frequency of attacks against information resources of the organization (Bagchi and Udo, 2003; Computer Emergency Response Team (CERT), 2004; Gordon et al., 004).According to some estimates, the number of reported incidents to the US CERT between 1998 and 2003 have nearly been doubled each year with nearly 137,529 incidents alone in 2003. According to an Ernst and Young survey, security incidents can cost organizations from $17 to 28 million for each occurrence (Garg et al., 2004).As the incidents are normally frequent and expensive, therefore management has to take security as seriously as possible in order to keep safe critical organizational information. For years, security authorities documented that security problems require managerial attention to solve them. (Allen, 1968; Parker, 1981; Van Tassel, 1972).Even then, managers usually did not pay more attention to the importance of security and many allow their information systems (IS) to be either protected in a light manner or totally open to attack(Straub, 1990).During 1990s some of the key issues regarding security were altogether eliminated from the top 20 list (Brancheau et al.,1996).Managerial attention towards information security still appears to be inadequate in spite of amplified media attention about e-mail viruses, internet worms, and software vulnerabilities since 2000. According to one key issue in 2004, in which more than 874 certified information security professionals showed that top management help and support was ranked number one from the list of 25 security issues. Similarly, organizational culture ranked at sixth number and policy-related issues ranked seventh (Knappet et al., 2004).There are hardly few studies that have developed and pragmatically-tested theoretical models that apply these managerial paradigms to information security (Kankanhalli et al., 2003; Straub, 1990).Few of the IS scholars even perceived grave need of empirically based information security research (Kotulic and Clark, 2004). There is need to explore, develop, and empirically test a theoretical form in information security.Many analysts consider that the biggest threat to information security is human being which should be addressed as soon as possible (Da Veiga, Martins, & Eloff, 2007; Von Solms, 2000,1997). More attention should be given to the information security culture within the organization (Von Solms, 2000). Information security should be practiced on everyday basis in order to inculcate the true spirit of it in the organizational culture (Martins & Eloff, 2002). The leader should recognize the seriousness of external threats from dynamic global competition, enhanced regulations and political intervention coupled with the prudence to see and evaluate the future in its broader prospective with due responsibilities (Benbow1995).

1.4. Security Breaches:

Various independent surveys show that in 2002, there were 36 to 90 percent computer security breaches in organization. (Bosworth, S., Kabay, 2002). Such security incidents are increasing spending on IT security, which reached to nearly $ 30.3 billion by 2005. (Ernst & Young, LLP ,2006).The information security breaches survey conducted by Price Waterhouse Coopers (PWC, 2004) stated that technology related issues such as system failure and data corruption are at the peak. It further elaborated that human error is main factor for security breach. The solution for it is to create a security-aware culture and human interaction leads to fraud or social engineering. So good information security governance should be deployed (Von Solms, 2006).

1.5. Security of organization's information system (IS):

Information system is of critical importance to gain the competitive advantage. Competencies in the area of IS are getting much importance and concern in organizations (Quinn & Paquette, 1990).The aim of IS security is to keep an organization's information and knowledge resources-information, data, hardware and software secure (Pathak 2000b).The present changing world has too changed the societal expectations regarding access to information, confidentiality, and disclosure. These emerging changes present challenges in relation to the traditional ones for privacy and confidentiality of personal information In hospital especially, if information to communicate fails to convey to the patients then problems for of care arises out of it (Northamptonshire Health Authority & Northamptonshire Social Services, 1999).ISO/IEC 17799 2005) provides with guidelines and recommendations regarding information security. It also tells about some of the standards for information security. The following 11 control sections in table briefly explain the information security with all its relevant parapemeters.

	Components of Information Security
1	**Security policy** that aims to provide management direction and support for information security, including laws and regulations.
2	**Organization of information security** that constitutes the process implemented to manage information security within the organization.
3	**Asset management** that focuses on asset inventories, information classification, and labeling.
4	**Human resources** security that considers permanent, contractor, and third-party user responsibilities to reduce the risk of theft, fraud, and misuse of facilities. This section also includes awareness, training, and education of employees.
5	**Physical and environmental** security controls that allow only authorized access to facilities and secure areas.
6	**Communications and operations management** that focus on the correct and secure operation of information processing facilities, such as segregation of duties, change management, malicious code, and network security.
7	**Access controls** that manage user access to information and include clear desk principles, network access controls, operating system access controls, passwords, and tele-working.
8	Information **systems acquisition, development, and maintenance** that ensure the security of user-developed and off-the-shelf products.
9	Information security **incident management** that ensures that incidents are communicated in a timely manner and that corrective action is taken.
10	**Business continuity management** that focuses on business continuity plans and the testing thereof.
11	**Compliance** in terms of statutory, regulatory or contractual, laws, audit and organizational policy requirements, or obligations.

TABLE 1 Control Sections of ISO/IEC 17799 (Adapted from ISO/IEC 17799, 2005)

The research conducted by Eloff and Eloff (2005) concluded that PROTECT is aimed at addressing all the key issues of information security. This may include Policies, Risks, Objectives, Technology, Execute, Compliance, and Team. The table 2 shows control components of Protect which are given below;

	Control Components of PROTECT
1	The **policy** component includes information security policies, procedures, and standards, and leading guiding rules for keeping these.
2	**Various Risk** methodologies to identify system vulnerabilities are covered in the risk component.
3	**Objective** refers to Protection i.e. to minimize risk by maximizing security through vigilant monitoring
4	**Technology** refers to hardware, software, and systems product components of the IT infrastructure and, where possible, the use of certified products.
5	Information security controls need to be established, maintained, and managed.
6	The **compliance** component covers both internal compliance with the organization's policies and external Compliance with information security expectations set by outside parties to the organization. Compliance also includes international codes of practice, legal requirements, and international standards.
7	**Team** refers to the human component, namely all the employees of the organization, where each has a responsibility towards securing information. The objective is to create a security-aware workforce that will contribute to an improved information security culture.

TABLE 2 Control Components of PROTECT (Adapted from Eloff & Eloff, 2005)

The Capability Maturity Model (McCarthy & Campbell, 2001) approach gives various security controls mechanism for the protection of information assets against unauthorized access, modification or destruction. There are seven control levels that are portrayed in table 3 which are given as below;

	Controls Levels of the Capability Maturity Model
1.	**Security leadership:** Security sponsorship/posture, security strategy, and return on investment/metrics.
2.	**Security program**: Security program structure, security program resources, and skill sets.
3.	**Security Policies**: Security policies, standards, and procedures.
4.	**Security Management**: Security operations, security monitoring, and privacy.
5.	**User Management**: User management and user awareness.
6.	**Information Asset Security:** Application security, database/meta security, host security, internal and external network security, anti-virus, and system development.
7.	**Technology Protection & Continuity**: Physical and environmental controls and continuity-planning controls.

TABLE 3 Controls Levels of the Capability Maturity Model (Adapted from McCarthy & Campbell, 2001)

In order to mitigate risk the following five principles of Tudor (2000) are essential for the protection of organization data to be secured against all the threats. These five principles are the back bone which ensure the reliable and confidential flow of information among individuals in specific realm.

The table 4 below shows these principles of the information security architecture as;

	Principles of the Information Security Architecture
1.	**Security organization and infrastructure:** Roles and responsibilities are well explained
2.	**Security policies, standards, and procedures**: Policies, standards and procedures are developed..
3.	**Security program:** A security program is compiled taking risk management into account.
4.	**Security culture awareness and training:** Users are trained to cater the relationship of trust with all the stakeholders.
5.	**Monitoring compliance:** Internal and external monitoring of information security is conducted.

TABLE 4 Principles of the Information Security Architecture (Adapted from Tudor, 2000)

2. Information security in Health sector:

According to the professional conduct of doctors, they are supposed to maintain confidence with the patients, while misuse of confidential medical information is a vital professional misconduct. Information of the patients is confidential to that patient and should never be divulged, unless, exceptionally, it is required for some legal purpose (General Medical Council, 2000). Each use of the patient identifiable information should be of lawful purpose and the person handling this activity must be held responsible for it(Department of Health, 1997)It must be held that confidentiality of patient information in not breached other than in exceptional circumstances (McLelland & Thomas, 2002**).** The Caldicott Report (1997) identifies three steps for the optimum level of security and privacy of patient health information, which are as below; improving the cultural consciousness on issues of confidentiality

a. build up organizational framework for access to and of the utilization of patient information
b. privacy enhancing technologies should be developed

The patient identity should not be disclosed to third party without the free consent of patient otherwise there would be breach of confidence (Court of Appeal, 2000).The implementation of policies and procedures essential for the protection of patient's privacy must be topmost priority of organization. Serious issues arise of data security, confidentiality and ethics when the patient information is used for secondary purpose (NHS Executive, 1998).

Addressing Security Issues:

Security can not possible with single measure rather it's the combination of various parameters to be tackled (Applegate, et al., 2003). Elements of security comprise the following points (Bolles, Gary A, 2006);

1. Security Polices: it includes all the documentary brief of what is expected of the employees.
2. Firewalls: it prevents all the unauthorized and illegitimate users from using information
3. Authentication: its make possible by passwords for users
4. Encryption: in some cases this technique is used in order to make sure that the information may not be extracted by the intruders. There are many points which should be focused while managing security for the data to be Protected (Olson, David L, 2004);

1. Make deliberate security decisions

2. Consider security as a moving target
3. Change management be disciplined
4. Educate users
5. Inculcate multiple level of technical measures

3. HYPOTHESIS

The following are the hypothesis developed from the study;

- Effective Leadership concerns almost equally for PEOPLE as well as TASK.
- Effective Leadership Style and its impact on Information security is POSITIVELY Correlated.

4. METHODOLOGY

4.1. Sample

A questionnaire was given to 185 respondents in 155 Hospitals across major cities of Pakistan. The cities we have covered are; Karachi, Lahore, Islamabad, Peshawar, Hyderabad, Larkana, Khairpur, Sukkar, Dera Ismail Khan, Bannu, Sarai Naurang, Karak, and Tank. A total of 107 respondents from 73 Hospitals filled the questionnaire. All the questions were in the Likert style in order to ease the respondents for his/her responses. The respondents were mainly Doctors and Administrators of the hospitals. We have done it because we were interested to gather data from their own point of views and perceptions regarding the same organization.

4.2. Software Tool

For analysis and accurate output SPSS and MS Excel were used. Through this software tools we come to know about the statistical measurement and analysis about our data of questionnaire.

4.3. Questionnaire Format

There were nineteen questions in all. Twelve of the questions i.e. seven were related to the Leadership specificity towards PEOPLE while five questions were for the Leadership specificity towards TASK and seven questions were for Information security. These seven questions in all were to support the effect of leadership style on information security. The main aim of such arrangement was to know the Leadership through Blake and Mouton Leadership Grid by putting the resultant data on Y-axis and X-axis and the impact of leadership style on information security. The format of the questionnaire was simple. All the questions were put in likert style format in order to facilitate our respondents for their time saving and less labor. The scaling of the questions was from 1. To 5.i.e. from Strongly Agree to Strongly Disagree respectively.

4.5. RESULTS OR FINDINGS

The following table shows the whole results of the twelve questions with their due analysis.

Independent Variables	*Mean*	*St: Deviation*	*Mode*
People Oriented:			
Participation of employees in decision making and to implement their ideas and suggestions are important.	**1.66**	**.752**	**1**
I enjoy coaching people on new tasks and procedures.	**1.64**	**.484**	**2**
When correcting mistakes, I do not worry about jeopardizing relationships.	**2.14**	**.895**	**2**
I enjoy explaining the intricacies and details of a complex task or project to my employees.	**1.95**	**1.004**	**2**
Nothing is more important than building a great team	**1.82**	**.684**	**2**
I honor other people's boundaries.	**2.13**	**1.332**	**2**
Counseling my employees to improve their performance or behavior is second nature to me.	**2.01**	**1.005**	**2**
Task Oriented:			
Nothing is more important than accomplishing a goal or task.	**1.51**	**.502**	**2**
I monitor the schedule to ensure a task or project will be completed in time.	**1.69**	**.745**	**1**
When seeing a complex task through to completion, I ensure that every detail is accounted for.	**1.81**	**.392**	**2**
Easy to carry out several complicated tasks at same time.	**2.48**	**1.152**	**2**
Breaking large projects into small manageable tasks is second nature to me.	**1.99**	**.986**	**2**
Information security Related:			
Our organization has an information security policy	**3.00**	**1.197**	**4**
Our organization takes steps to prevent unauthorized access of organization's premises	**2.50**	**1.269**	**1**
We take information security as an agenda item at regular senior management meetings	**2.86**	**.936**	**2**
The employees who violate the security policy subject to a disciplinary process.	**2.31**	**.503**	**2**
The information leakage is dominant in those organizations where the interaction between senior management and employees are not cooperative	**2.33**	**1.114**	**1**
Our organization takes steps to inculcate the values of loyalty and sincerity in employees in order that secrecy of information may not be divulged	**2.54**	**1.012**	**2**
We have assigned specific authorization and authentication for information system's users	**2.34**	**.739**	**3**

Table 5. Results/Findings against questionnaire questions

The above results from the respondents clearly show that most of them are in the agreeable region to the aforementioned scenario of questions i.e. the Mean for all questions are in the range from 1.50 to 2.50. Similarly it's also evident from the Mode that most of the respondents have clicked 2 most of the time, which show Agreement with the scenario of the aforementioned questions. While in information security, there are mix responses from the respondents. The correlation of the information security questions with leadership style questions show positive relationship and dependency. This would be very clear when we cross tabulate the results of information security related questions with that of leadership questions in the below given tables. Prior to go there, it's mandatory to know the leadership matrix and the prevalent leadership style in Pakistan. From the respondents' feedback, it has been concluded that all of them consider the Team Leader is the most prevalent in Health sector (Hospital) of Pakistan.

The following Diagram (i.e. figure 2) shows the overall result.

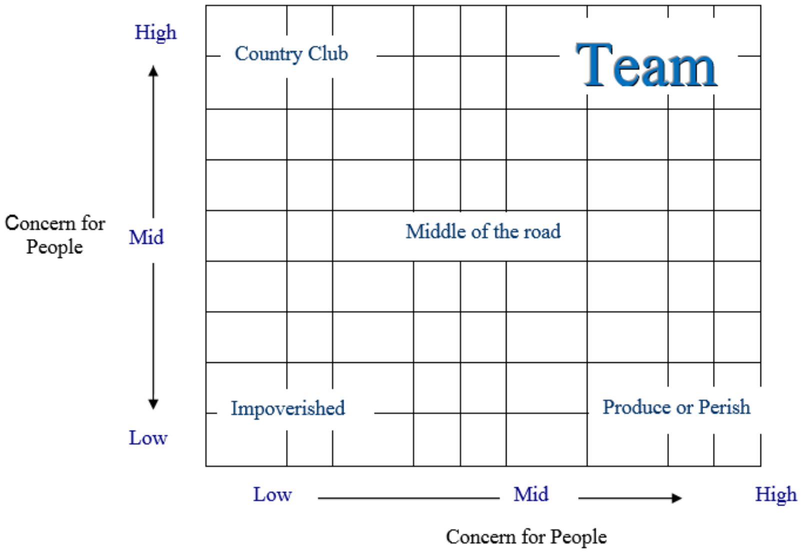


Figure: 2. the overall result/finding of the survey

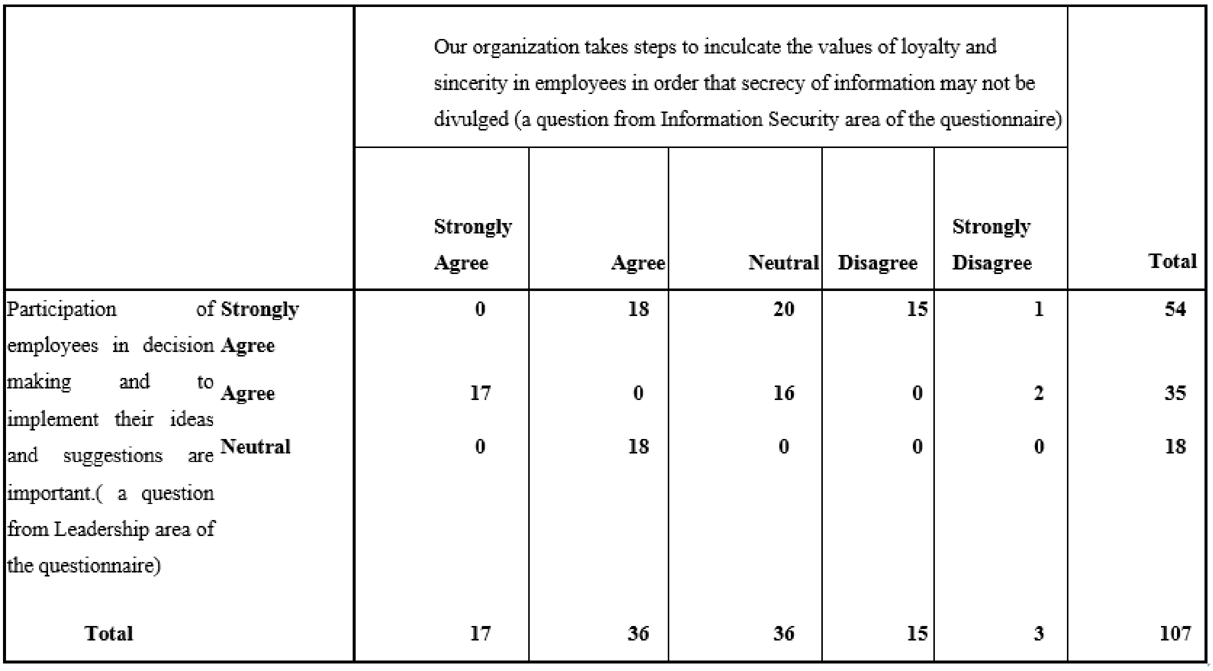
On the basis of our findings from the Mean values of the questionnaire, it has been concluded that the Team Leadership is the most prevalent Leadership style in health sector (i.e. Hospitals) of Pakistan. This result has been acquired by assuming 1 and 2 for High, 3 for Mid and 4 and 5 for Low concerns on the basis of the questionnaire pattern.

By taking cross section of Mean values of Production and People, it clearly indicates the region of Team leadership. If we have a look on the accumulative mean results of the questionnaires then most of the means of both Production and People lie between 1 and 2 which indicate a region of High Concern for Production as well as People (i.e. 1 for strongly agree and 2 for Agree). This result clearly shows that most of the respondents out of total 107, consider that in Pakistan there is Team Leadership style in hospitals of Pakistan.

4.6. Leadership impact on Information Security (Cross Tabulations)

The relationship of Leadership with Information security can be easily seen through the cross tabulations of many questions from Leadership and Information Security related areas.

Participation of employees in decision making and to implement their ideas and suggestions are important.
*** Our organization takes steps to inculcate the values of loyalty and sincerity in employees in order that secrecy of information may not be divulged**

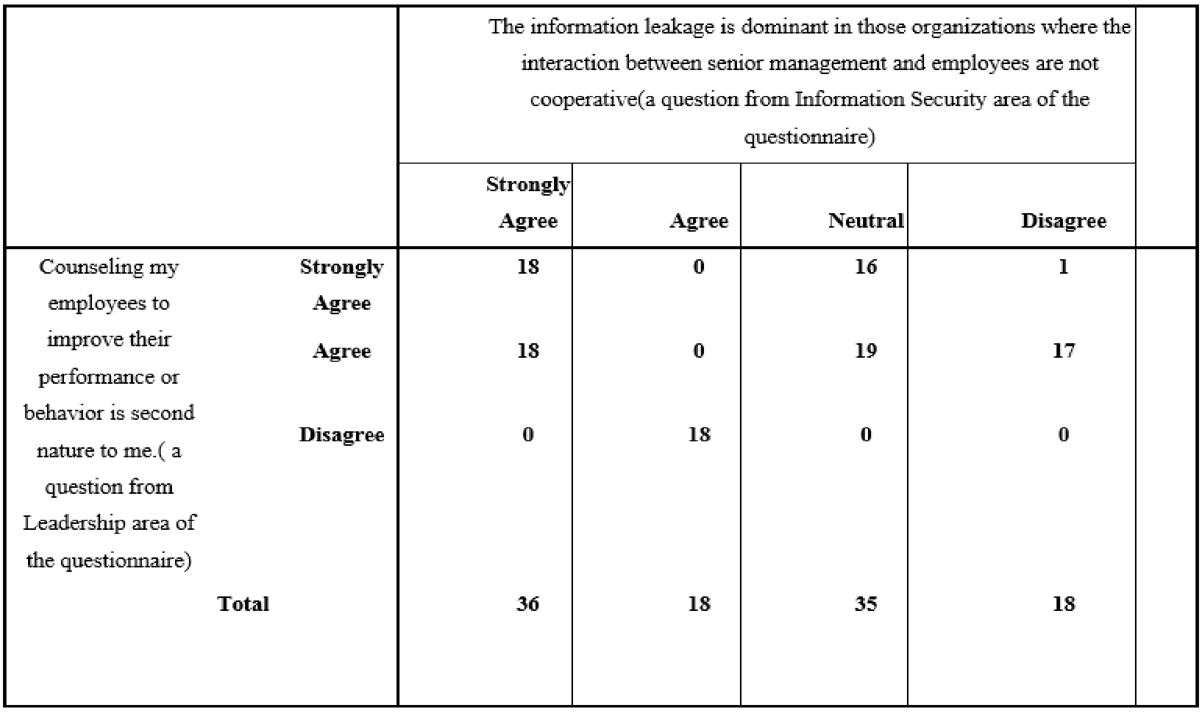


		Our organization takes steps to inculcate the values of loyalty and sincerity in employees in order that secrecy of information may not be divulged (a question from Information Security area of the questionnaire)					
		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Total
Participation of employees in decision making and to implement their ideas and suggestions are important.(a question from Leadership area of the questionnaire)	Strongly Agree	0	18	20	15	1	54
	Agree	17	0	16	0	2	35
	Neutral	0	18	0	0	0	18
Total		17	36	36	15	3	107

Table 6. cross tabulation of one of the leadership characteristic and Information attribute

From the above table it has been clear that both of scenarios are interrelated with each other and both have shown greater tendency towards agreeable region (i.e. strongly Agree plus Agree). In other words we can say that the values of sincerity and loyalty to maintain the secrecy mainly related with the employee role in participating in decision making. This shows that the Participation role make them more trust worthy and reliable for keeping all the secret information. Similarly the other interrelation between the Leadership and Information Security through cross tabulation is as follow;

Counseling my employees to improve their performance or behavior is second nature to me * The information leakage is dominant in those organizations where the interaction between senior management and employees are not cooperative



		The information leakage is dominant in those organizations where the interaction between senior management and employees are not cooperative(a question from Information Security area of the questionnaire)				
		Strongly Agree	Agree	Neutral	Disagree	
Counseling my employees to improve their performance or behavior is second nature to me.(a question from Leadership area of the questionnaire)	Strongly Agree	18	0	16	1	
	Agree	18	0	19	17	
	Disagree	0	18	0	0	
	Total	36	18	35	18	

Table 7. cross tabulation of leadership style and information security

This table too shows the relationship between the aforementioned questions' scenario in a positive manner. We can say that counseling with employees is vital to avoid the Leakage of valuable information of the organizations. Hence the above findings show an agreeable correlation with each other. So it's prudent to have the entire employees in full confidence by counseling with them in order to increase performance and to avoid the leakage of secret information.

I monitor the schedule to ensure a task or project will be completed in time. * The employees who violate the security policy subject to a disciplinary process. Cross tabulation

Count

		The employees who violate the security policy subject to a disciplinary process.			
		Strongly Agree	Agree	Neutral	Total
I monitor the schedule to ensure a task or project will be completed in time.	Strongly Agree	0	34	17	51
	Agree	1	19	18	38
	Neutral	1	17	0	18
Total		2	70	35	107

Table 8. Cross tabulation of leadership style and information security

Having a look at the above cross sectional table- 8 ,its obvious to note that on one hand monitoring the schedule through its completion has greater relation with the employees who violate the predefined rules are subject to disciplinary process of the organization. In our case, majority of the respondents consider that there is strong correlation between the aforementioned two given scenarios. From the above graph, there is high inclination towards acceptance realm as compared to be neutral or disagree. So our overall discussion means that there is positive or strong correlation between the given two scenarios.

6. CONCLUSION

From the aforementioned discussion, we come across a conclusion that Team leadership is the most prevalent Leadership style in Health sector (i.e. Hospitals) of Pakistan. It is clearly shown in the figure 2 above by cross-section two lines of People and task Oriented approach through Team Leader’s quadrant at the symbol “star” representing the cross-section of 8.93 and 5.5. So the overall survey clearly shows that Team Leadership is the most prevalent style of Leadership with greater emphasis on care for the relationship with the employees but with not that much emphasis on the task as well. In short we can say that the leaders are more concern with People as compared to task. Although the Task orientation is above the middle of the road yet one can say that the more concentration is on relationship with the employees for their needs, requirements and the like.

It has also been known that Leadership has its impact on information Security. From the cross tabulation we can conclude that information security is related with the leadership phenomenon and at specific to the particular leadership style. Although the other types of leadership styles are also in place with the nature of situations and requirements yet all the successful organizations use the aforementioned most prevalent style.

References:

Allen, B. (1968), "Danger ahead! Safeguard your computer", *Harvard Business Review*, November/December, pp.97-101.

Applegate, Lynda M., Robert D. Austin, and E. Warren McFarlan. Corporate Information Strategy and Management, 6th Ed. New York, NY: McGraw-Fiill/Irwin, 2003.

Alvesson, M.,Organisationskultur och ledning, Liber ekonomi, Malmö,2001.

Anderson, R. (1995) NHS-wide networking and patient confidentiality, BMJ, 311, 5–6

Benbow, N. (1995), "Preparing for tomorrow", Executive Development, Vol. 8 No.7, pp.29-30.

Bolles, Gary A. "Technology: Optimization," CIO Insight, 1 Sept. 2003. Available at www.cioinsight.com/print_article/0,3668,a=61644,00.asp (accessed 7 June 2006

Bagchi, K., Udo, G. (2003), "An analysis of the growth of computer and internet security breaches", *Communications of the Association for Information Systems*, Vol. 12 No.46, pp.1-29.

Beauchamp, T. L. & Childress, J. F. (1994) Principles of Biomedical Ethics. Oxford: Oxford University Press

Brancheau, J.C., Janz, B.D., Wetherbe, J.C. (1996), "Key issues in information systems management: 1994-95 SIM results",*Management Information Systems Quarterly*, Vol. 20 No.2, pp.225-42.

Bosworth, S., Kabay, M.E. (Eds),Computer Security Handbook, 4th ed., John Wiley, New York, NY, (2002),

Boal,K.B, Hooijberg,R., “strategic leadership research: moving on”, in the leadership quarterly yearly review of leadership, 11(4),2001,pp.515-550.

Business dictionary, information security, access on November 2008 http://www.businessdictionary.com/definition/information-security.html

Court of Appeal (2000) Regina v Department of Health, ex parte Source Informatics Ltd. Times Law Reports, 18 January, 17–18

Computer Emergency Response Team (CERT) (2004), "CERT statistics", available at: www.cert.org/stats/cert_stats.html#incidents (accessed May 2004)

D. Goleman, “leadership that gets results”. Harward Business Review. Vol. 78.N 2.pp. 78-90,2000

Da Veiga, A., Martins, N., & Eloff J. H. P. (2007). Information security culture—validation of an assessment instrument. Southern African Business Review, 11 (1): 147–166.

Department of Health (1997) The Caldicott Committee Report on the Review of Patient-Identifiable Information. London: Department of Health.

E. Ogbonna, L.Harris, “Leadership style, organizational culture and performance: Empirical evidence from UK companies”. International Journal of Human Resource Management vol.11N4, pp.766-788, 2000

Eloff, J. H. P. & Eloff, M. (2005). Integrated Information Security Architecture, Computer Fraud and Security, 2005 (11), 10–16.

Ernst & Young, LLP (2006), Global Information Security Survey, .

G.Evkall, L.Ryhmmar. “Leadership style, social climate and organizational outcomes: A study of a Swedish University college”. Creativity and innovation Management. Vol.7.N.3.pp. 126-130. 1997

Garg, A., Curtis, J., Halper, H. (2004), "Quantifying the financial impact of IT security breaches", Information Management & Computer Security, Vol. 11 No.2, pp.74-83.

General Medical Council (2000) Confidentiality: Protecting and Providing Information. London: GMC

Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R. (2004), *2004 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, San Francisco, CA,

Grid International, Inc. http://www.gridinternational.com/gridtheory.html

Information security, access November 2008, http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542----000-

ISO/IEC 17799 (BS 7799-1) (2005). Information technology. Security techniques. Code of practice for information security management, Britain.

ISO/IEC 27001 (BS 7799-2) (2005). Information technology. Security techniques. Information security management systems—requirements,Britain.

Jeffrey Gandz, Reprint # 9B05TA01 IVEY MANAGEMENT SERVICES •

January/February 2005 COPYRIGHT 2005

JPL ethics program, access November 2008 http://ethics.jpl.nasa.gov/resources/d-info_security.html

Kankanhalli, A., Hock-Hai, T., Bernard, C.Y.T., Kwok-Kee, W. (2003), "An integrative study of information systems security effectiveness", International Journal of Information Management, Vol. 23 pp.139-54.

Knapp, K.J., Marshall, T.E., Rainer, R.K., Morrow, D.W. (2004), *Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC)2 Survey Results*, Auburn University, Auburn, AL, .

Kotulic, A.G., Clark, J.G. (2004), "Why there aren't more information security research studies?", *Information & Management*, Vol. 41 No.5, pp.597-607.

Lok, P. and Crawford, J. 2004. The effect of organisational culture and leadership style on job satisfaction and organisational commitment: A cross-national comparison. The Journal of Management Development; Volume 23 No. 4.

Mind Tools Ltd, 1995-2009 http://www.mindtools.com/pages/article/newLDR_73.htm

Mosadeghrad, A.M. (2003a), "The role of participative management (suggestion system) in hospital effectiveness and efficiency",Research in Medical Sciences, Isfahan, Vol. 8 No.3, pp.85-9.

Mosadeghrad, A.M. (2004), The Handbook of Hospital Professional Organization and Management, Dibagran Tehran, Tehran, Vol. 2.

McClelland, R. & Thomas, V. (2002) Confidentiality and security of clinical information in mental health practice. Advances in Psychiatric Treatment, 8, 291–296

Martins, A. & Eloff, J. H. P. (2002). Information Security Culture. In Security in the information society. IFIP/SEC2002. (pp. 203–214). Boston: Kluwer Academic Publishers.

McCarthy, M. P. & Campbell, S. (2001). Security Transformation. McGraw-Hill: New York.

Mumford, A. (1994), "Four approaches to learning from experience", *The Learning Organization*, Vol. 1 No.1, pp.4-10.

NHS Executive (1998) Information for Health: An Information Strategy for the Modern NHS 1998–2005. A National Strategy for Local Implementation. London: Department of Health.

Northamptonshire Health Authority & Northamptonshire Social Services (1999) The Independent Inquiry into the Care and Treatment of Wayne Licorish. Northampton: Northamptonshire Health Authority

Ogbonna, H.E. and Harris C.L. 2000. Leadership style, organizational culture and performance. Int. J. of HRM, Aug 2000.

Olson, David L. Managerial Issues of Enterprise Resource Planning Systems. New York, NY: McGraw-Hill/Irwin, 2004.

Parker, D.B. (1981), *Computer Security Management*, Reston Publishing Company, Reston, VA,

PriceWaterhouseCoopers. Information Security Breaches Survey. (2004). Retrieved 12 March 2005 from http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

Pathak, Information Security Forum (ISF), "The forum's standard of good practice"http://www.isfsecuritystandard.com November 2000

President (2003), "National strategy to secure cyberspace", available at: www.whitehouse.gov/pcipb (accessed May 2004),

Quinn, J. B., & Paquette, P. C. (1990). Technology in services: Creating organizational revolutions. Sloan Management Review, winter, 67–78.

Robert Kreitner, Angelo Kinicki, and Book: Organizational Behavior—international edition,sixth edition,

Research Concepts, LLC (2002), "Trends in the Networked World", 2002 Network World 500 Research Study, .

Straub, D.W. (1990), "Effective IS security: an empirical study", *Information Systems Research*, Vol. 1 No.3, pp.255-76.

S.Kahani, J.Sosik. "Effects of leadership style and folower's cultureal orientation on performance in group and individual task conditions ". Personal Psychology. Vol. 50. N, pp. 121-147. 1997

The Caldicott Committee Report on the Review of Patient-Identifiable Information. London: Department of Health.(1997)

Tait, R. (1996), "The attributes of leadership", *Leadership & Organization Development Journal*, Vol. 17 No.1, pp.27-31.

Taylor, R., Taylor, C. (1996), "Trouble at the top: assessing the upper-level executive", The Journal of Workplace Learning, Vol. 8 No.7, pp.13-15.

The leadership Grid Source: From R. Blake and A Adams McCanse, Leadership Dilemmas-Grid Solutions, p.29, copyright 1991 by Robert R Blake and the estate of Jane S Mouton. (Published in book title: Organizational Behaviour by Robert Kreitner and Angelo Kinicki, chapter 17-Leadership)

Tudor, J. K. (2000). Information Security Architecture—An integrated approach to security in an organization. Boca Raton, FL: Auerbach.

Ulukan, C. (2005). Managerial issues in open and distance education organizations in transition: A need for systematic approach. Turkish Online Journal of Distance Education-TOJDE, 6 (2). Retrieved February 22, 2007 fromhttp://tojde.anadolu.edu.tr/tojde18/articles/article8.htm

Van Tassel, D. (1972), Computer Security Management, Prentice-Hall, Englewood Cliffs, NJ, .

V. Vroom,, "Leadership and decision making process",organizational Dynamics. Vol. 28, N4,pp.82-94,2000

Von Solms, R. (1997). Driving safely on the information superhighway. Information Management & Computer Security, 5 (1), 20–22.

Von Solms, B. (2000). Information security—The third wave? Computers and Security, 19(7). November, 615-620.

Von Solms, S. H. (2006). Information Security—The fourth wave. Computers and Security. 25 (2006), 165–168.

What is managerial grid? Access on November 19,2008 http://www.12manage.com/methods_blake_mouton_managerial_grid.html