Journal of Theoretical and Applied Information Technology
10th February 2016. Vol.84. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A PERCEPTUAL STUDY ON FACTORS OF MEDICAL DATA SECURITY IN INDIAN ORGANIZATIONS

NIRMALYA CHAKRABORTY, DR. (MS) VANDNA SHARMA, DR. (MS) JAYANTHI RANJAN

Global Lead (IT Risk Management), Capgemini India Pvt. Ltd.
, Head (Management Studies), Birla Institute of Technology, Meshra
, Head (International Relations) Institute of Management & Technology, Noida
E-mail: nir.engg@gmail.com

ABSTRACT

Objective of the research: Risk management in the IT world is quite a complex, multi faced activity, with a lot of relations with other complex activities (Rainer et al, 1991; Bahli and Rivard, 2005). The purpose of the study is to find out the major factors impacting medical data security in the Indian organizations.
Current state of Research Area: Information security awareness is considered very vital because of the fact that security techniques as well as procedures are vulnerable to misuse and non-usage by the end users (see Ceraolo, 1996; and Straub, 1990). Medical data too is a crucial element of the overall information system of an organization. Any breach in the security of medical data may have detrimental effects on the organizations. Straub and Welke (1998) have argued that security breaches are far more regular and destructive than it is usually though to be. This is mainly because of the fact that the managers are generally not concerned with issues related to information security and unaware of the nature of risk. Thus there exists an immediate need to secure medical data and ensure its reliability and availability at the right time and to the right person.
Methodology: For the quantitative study a survey has been conducted with the help of a close ended questionnaire. The responses were collected from employees of companies operating in the Healthcare, Telecom industry, and IT industry in India. The questionnaire was circulated in the physical mode. Convenience sampling was deployed in order to select the respondents. The validity of the constructs was assessed by means of factor analysis. Descriptive as well as inferential statistics like t-test, ANOVA have been used for obtaining the desired results.
Conclusion : The study also highlighted that there are multiple constructs that should be considered while measuring the overall information security within an organization. These constructs or factors should be evaluated both individually as well as collectively in order to make the information secure and reliable.
Limitations: One of the biggest limitations of the current study is that it is confined to only three sectors namely Healthcare, Telecom & IT. Further we have studied only one country i.e. India.
Scope for further Research: medical data management practices in advanced as well as in emerging economies differ a lot. Such differences can be studied to provide a comprehensive framework of medical data management.
Keywords: *Medical Data, Risk Analysis, Factor Analysis, Information Security*.

1. INTRODUCTION:

Risk management in the IT world is quite a complex, multi faced activity, with a lot of relations with other complex activities (Rainer et al, 1991; Bahli and Rivard, 2005). Information security awareness is considered very vital because of the fact that security techniques as well as procedures are vulnerable to misuse and non-usage by the end users (see Ceraolo, 1996; and Straub, 1990). Medical data too is a crucial element of the overall information system of an organization. There is currently a very large shift in interest from paper-based medical records to electronic based records. These efforts are implemented by various organizations around the world. This has given rise to the concept of electronic health records (EHR) which is gaining immense attention in the current business era (Fernández-Alemán et al., 2013). Recent studies point out that an integrated medical record can provide various benefits including cost reduction, quality improvement in providing care, promotion of evidence-based healthcare and mobility (see Greenhalgh et al., 2010; Allard et al., 2010).

Ownership of the medical data is also now a serious concern (Sunyaev et al, 2010). Whether data ownership stays with the company or with the employee (due to its sensitivity) is also a debated question (see Denton, 2001; McGee, 2008; Swartz, 2008). One of the most important aspects related to privacy in handling medical data is the application of various standards and regulations. Different countries and regions have different regulations pertaining to the security as well as the privacy of medical data. The major regulations related to medical data include HIPPA in the US, Data Protection Directive 95/46/EC in the European Union, the Privacy Code applicable in New Zealand, and certain other. These regulations generally provide guidelines related to the anonymity as well as the accessibility of the medical data. In the US, the healthcare data is protected by the Health Insurance Portability and Accountability Act[1] (HIPAA) of 1996. HIPAA ensures that Protected Health Information (PHI) is secured whose failure can result in significant damage and penalties. Any breach in the security of medical data may have detrimental effects on the organizations. Straub and Welke (1998) have argued that security breaches are far more regular and destructive than it is usually thought to be. This is mainly because of the fact that the managers are generally not concerned with issues related to information security and unaware of the nature of risk. Thus there exists an immediate need to secure medical data and ensure its reliability and availability at the right time and to the right person.

2. THEORETICAL CONTEXT

In this section we systematically review various studies that describe the challenges confronting the security of medical records held by employers and how employers go about managing these issues. This section also reviews the major themes related to security concerns of employees' medical records and classifies the themes into six broad categories.

Dhillon and Backhouse (2001) have done a comprehensive literature review related to information security. Based on their review and deriving comparisons from a social and philosophical framework, the authors have classified security research into four different paradigms. These include interpretive, radical humanist, functionalist and radical structuralist. The authors have also advocated that in order to understand information security issues a socio-organizational theory should be used. This is because most of the information security technologies are maintained, designed and used by human beings in the organizations.

Stallings and Brown (2008) have defined information security as security provided to an information system for the purpose of attaining the objectives of protecting the confidentiality, availability as well as the integrity of information system. Goodhue and Straub (1991) have conducted a qualitative survey in order to develop a model consisting of managerial perceptions regarding various risks involved in information security.

2.2 Information Security And Regulatory Compliance

One of the most important aspects related to privacy in handling medical data is the application of various standards and regulations. Different countries and regions have different regulations pertaining to the security as well as the privacy of medical data. The major regulations related to medical data include HIPPA in the US, Data Protection Directive 95/46/EC in the European Union, the Privacy Code applicable in New Zealand, and certain other. These regulations generally provide guidelines related to the anonymity as well as the accessibility of the medical data. There have been various studies done related to the role of these regulations in maintaining the security of medical data (see Neubauer and Heurix, 2011; Kwon and Johnson, 2013; Kahn and Sheshadri 2008; Elger et al., 2010; Reis et al., 2008; Hembroff et al., 2010).

Kwon and Johnson (2013) have tried to study how information security performance and compliances impact one another. They have also

[1] The HIPA Act was passed by the US Congress in the year 1996. It is also generally known as the Kennedy–Kassebaum Act. The Title I of the act is related to protecting the insurance coverage of workers as well as their families in case of job loss. The Title II of the act requires the establishment of various standards related to electronic transactions in healthcare information.

tried to find out how security resources contribute to data protection as well as regulatory compliance. The authors have collected data from a survey conducted on 243 hospitals. The respondents to the survey included executives from the IT department, security officers, privacy officers, and compliance officers. The authors have applied Simultaneous Equations Modeling (SEM) technique for their research. The authors found that the impact of security resources differ for data breaches and perceived compliance. The authors also found that security operational maturity plays a vital role in the outcomes. These results imply that for operationally mature organizations it is more likely that they get motivated by actual security performance rather than by meeting the compliances. On the other hand the immature organizations are likely to get motivated by meeting the compliances issues.

Hu et al. (2007) have made an attempt to comprehend how the external and internal influences impact the organizational actions towards the improvement of information systems security. The authors have presented a case study of an MNC and have analyzed the same from a neo-institutional theory's perspective. The authors found a significant presence of coercive and isomorphic processes. The authors also found that two forces, related to the internal environment, resist the initiatives of security improvements. According to the authors these two forces are work mobility's institutionalization and expected efficiency outcome's institutionalization. The authors also found out, with the help of the case, that though the regulatory forces act as powerful drivers for change there are other factors also which play a major role in influencing the organizational information security change.

Steinbart et al. (2012) have tried to investigate the interrelationships between information system security and internal audit functions. The authors have made use of semi-structured interviews taken from internal auditors as well as IT professionals. Based on the outcomes of these interviews, the authors have developed a model to explain the factors that influence the interrelationship between the functions of information security and internal audit. The authors found that the benefits of independent feedback about information security from internal auditors depend upon their level of understanding of IT functions.

Guo and Yuan (2012) have put forward and empirically tested a model in order to find out the impact of multilevel sanctions on preventing the workplace violations related to information security. The authors found that the two types of sanctions namely personal and workgroup sanctions significantly deter the employees from violating information security norms. The authors also found that the impact of organizational sanctions becomes insignificant when the impact of these two sanctions is taken into account.

Cox, Connolly and Currall (2001) have suggested that a web-based tutorial accompanied with a checklist can help in increasing the compliance to various policies in an academic environment. Many studies have also highlighted the ways in which organizational information security policies can be modified so as to improve the end user compliance (see Bulgurcu et al., 2010; Spears and Barki, 2010; D'Arcy et al., 2009).

2.2 Information Security Resources And Operational Maturity

Another major concern surrounding the security of medical data pertains to the operational maturity of the organization. If the information systems are operationally mature then the organization can preserve the integrity as well as the reliability of any information including employees' medical data. This also requires that the organization possess the necessary resources in order to implement the desired level of control mechanism. Various studies have been done in this area (see Doherty et al., 2009; Choe and Yoo, 2008; Lemaire et al., 2006; Sucurovic, 2010; Ruotsalainen, 2004).

Azaieza and Bierb (2007) have defined information system reliability as computers systems, consisting of hardware and software, which can perform their intended tasks without any interruptions. Farzandipour et al. (2010) have argued that the current advances in Information Technologies are posing newer threats to medical data stored in an electronic form. Haas et al. (2011) have argued that any electronic health record should have three primary security goals including confidentiality, integrity and availability (CIA).

Cremonini and Nizovtsev (2010) have made use of game theory setting in order to explain the interaction between attackers who want to gain access into the information systems and the defenders who want to prevent such an access. Their analysis showed that well-protected information systems can make use of signals to show their high level of protection. The authors have argued that this signaling can function as a deterrent tool for the attackers. The authors have argued that this is due to the fact that attackers want to derive financial benefits out of attacks on information security. This is possible in the cases where information security protections are weak.

Sammer (2010) has provided some guidelines to HR managers of various organizations related to the availability and utility of health care data of the employees. They have argued that insurers as well as other vendors of health care services have started making more data available. The HR executives should become more familiar with such type of data and should know clearly what they are looking for in this data. The author has further argued that a proper analysis of such data can help an organization in cutting the total health care expenses. The author has further claimed that the learnings form this data handling can enable the HR executives to apply the same techniques to other information as well.

There has been an increasing level of interest in research which focuses on the impact of computers in supporting co-ordination, communication and effective decision making (see Kraemer and King 1988; Sproull and Kiesler 1986). Solms (1999) in an article has contended that information systems should make use of technically secure computers base which should be evaluated by certain quality norms. The author has also argued that this particular base should function in a secure environment. Wade and Hulland (2004) have argued that the current literature on IT neither provides a clear definition nor a clear conceptualization of various resources of information technology. Stanton et al. (2005) have argued that due to increased level of threats to information security systems both from external and internal sources, the significance of information security has become even more important.

Lichtenstein (1996) has identified a wide variety of issues that can be integrated in an acceptable use policy. The author has further categorized these issues into managerial, legal, operational, administrative, human and technical issues. Malvey et al. (2013) have tried to study the prevalence of the employee information sharing in various hospitals. They have also tried to analyze various factors that might impact the executives' willingness to share information related to employees. The authors found out that a there exists a culture of silence among various hospitals. This is because hospital executives generally tend to overestimate the probability of being used by their previous employees. The authors also found out that a few hospital executives may share negative information about their former employees but they generally do it off the record.

Tiwana and Konsynski (2009) have addressed the theoretically neglected relationship between information technology (IT) architecture in various organizations and their IT governance structure. They have studied the role of IT and its governance in determining the IT alignment. The authors have theoretically developed an idea that organizations' IT architecture modularity can helps them in sustaining IT alignment. This can be achieved by increasing the IT agility, and by decentralization of IT governance. The authors also argue that IT architecture complements the IT governance structure. The authors have also empirically testes their hypothesized mediated-moderation effects by using a data set consisting of 223 organizations. The empirical findings support the ideas developed by the authors.

2.3 Information Security Policies (Acceptable Use Policy)And Employee's Awareness

There is also a concern related to the internal policy and training of employees in order to enable them to properly handle the medical data. Several authors have raised these issues in their work (see Jafari et al., 2010; Schwager, and Anderson, 2008; Bouhaddou et al., 2012; Culnan et al., 2008).

Doherty et al. (2009) have argued that information security policy plays a leading role in promoting effective practices related to information security. Desman (2001) has provided a four stage procedure which can help in increasing the users' compliance to information security norms of the organization. These stages are (1) finding out the existing situation, (2) developing a baseline program, (3) communication of the program to the employees, and (4) evaluating and implementing the program.

Siau et al. (2002) have done a content analysis of acceptable use policy related to the internet usage in terms of various abuses covered in policy documents. The authors found that the most common issues related to acceptable use policy of internet included abuse of emails, unauthorized access, and violation of copyrights. Stephen and Petropoulakis (2007) have noted that an increasing number of employers are forced to discipline their employees due to the breach of organizational security policies by them. Foltz, Schwager, and Anderson (2008) have argued that for most of the organizations, the best way to control and monitor the behavior of their employees is by introducing an appropriate usage policy. Nolan (2005) has defined such usage policies as a set of guidelines and rules framed by the top management of IT department. These guidelines mention explicitly the manner in which companies' IT resources can be used by the employees. Attaran (2000) has contended that information system's acceptable use policy should clearly distinguish between the appropriate and inappropriate behaviors regarding the usage of organizational information resources.

Scott (1997) has highlighted the fact that acceptable use policy should play a critical role in minimizing the threats arising out of litigations faced by organizations. This can be accomplished by clearly explaining to employees the behaviors that are unacceptable and may lead to costly law suits for the organization. Doherty et al. (2011) have reviewed the acceptable use policy of various top ranking universities across the world. They found that the major role of any acceptable use policy currently appears as a tool to protect unacceptable behavior rather that acting as a proactive device in encouraging desirable behavior. The authors also found that currently there appears to be no coherent approach for dealing security related issues across various higher education institutes. Culnan et al. (2008) have argued that IT executives should help to secure the home computers of employees who opt for work from home option. This is because computers which are used at home are prone to increased level of threat to information security.

Various authors have suggested that any information security program should consist of a combination of various material including handouts, books, brochures, courses, newsletters, images, lectures, examples, videos, and reminders (see Murray, 1991; Peltier, 2000; Rudolph et al., 2002). Hadland (1998) has suggested that information security trainings should involve physical representation. The author has also suggested distribution of leaflets as a supporting material. Kajava and Siponen (1997) have proposed a procedure in order to maximize users' compliance to security norms especially in a university setting. Wood (2002) has strongly recommended a security education campaign in order to induce employees to follow information security norms. Lafleur (1992) has suggested that information security programs should contain two important components. These are (1) a promotional component which may include advertising and other material to remind the employees, and (2) a networking component which should help in achieving proper behavior from employees. Whitman et al. (2001) have contended that companies create information security policies in order to provide their employees with necessary guidelines describing the manner in which they can ensure security of information while they make use of information systems in their daily work lives.

Information security is viewed not just as a technical issue but also as a behavioral issue. There have been various studies conducted which have tried to identify the information security related behavior of the end users (see Siponen and Vance, 2010; Workman, Bommer, and Straub, 2008; Johnston and Warkentin, 2010; LaRose, Rifon and Enbody, 2008). Gowen et al. (2006) have tried to study the importance of strategic Human Resource Management (HRM) in controlling healthcare errors. The authors have also tried to find out the role of HRM in reducing health care errors, building better management processes and practices, and developing competitive advantage. The authors have used questionnaire to collect data. The sample size consists of directors of 587 hospitals of the US. The authors have made use of factor analysis as well as regression analysis. The authors found that there is a significant relationship between Strategic HRM and reduction in health care errors. The authors also found that there is a relationship between Strategic HRM and building better management processes and practices.

Muse et al. (2012) have investigated the relationship between the perceived value of traditional benefits as well as non-tradition benefits with the employee-employer relationship. They have also tried to find out how this relationship is linked to the job performance as well as turnover intentions. The authors have collected data from a random sample consisting of employees and their supervisors working at a healthcare organization. The sample size was of 457 respondents. The authors found out that non-traditional benefits are positively related to perceived organizational support. On the other hand the authors did not find the similar relationships between traditional health and financial benefits and perceived organizational support. The authors also found out that marital status acts as a moderator between the perceptions of non traditional benefits and organizational support.

Hedström et al. (2011) have argued that traditionally the information security management has been a control driven compliance model which assumed that behavior has to be controlled and regulated. The authors have proposed an alternate model in which multiple forms of rationality are assumed to be employed in the actions of organizations. The authors have further argued that due to these multiple forms of rationalities there can be potential conflicts of values. This can have a leading strategic impact on organizational performance. The authors have finally concluded that health care information management can be more efficiently managed by using the model proposed by the authors.

Liyanage and Egbu (2005) have tried to discover the function of facilities management in controlling the Healthcare Associated Infections (HAI). They have also made an effort to develop a three-dimensional approach that can be applied to control the HAI. The authors have used the interview method to collect data. They have collected data from 25 experts working in the infection control department at the National Health Service in Scotland. The authors found that integrating facilities management with core services is very important in avoiding duplication of work done by the healthcare employees.

Siponen (2000) has tried to develop a conceptual framework concerning information security awareness for employees of various organizations. He has based his work on various theories related to behavior and motivation. The author has also argued that persuasion strategy is more beneficial than monitoring strategy in increasing the commitment of users to security guidelines.

Mathieson (1991) has argued that Information security systems are useful to an organization only if the employees are aware of them and make use of them in their routine work.

Mitnick (2001) has argued that an ongoing information security awareness program should be conducted in order to influence employees to change their behavior.

2.4 Measurement And Evaluation Of Security Concerns

Many organizations are faced with the problem of how to measure the security and reliability of information system. This includes issues related to defining, measuring, communicating and monitoring various performance measurement criteria. This subsection provides a review of studies done in this area.

Atzeni and Lioy (2006) have suggested that information security measurement systems at any organizations should possess certain requirements. The authors have pointed out that these requirements include clarity, objectivity, brevity and ease of duplication. However some of these requirements are generally found to be missing in various measurement systems.

Wang (2005) has presented results of combined models of information security. He has suggested that the different components present in a system should be modeled separately. He has also suggested for using techniques like Markov chains and process algebra for various processes.

Torres et al. (2006) have found out 76 parameters that are spread across 12 very important success factors contained in the information security systems. These factors are found to be belonging to three different domains namely technology, people and process. The authors have also given a formula as well as measurement criteria for the various identified parameters.

Bartol et al. (2009) have discussed why it is important to quantify the security products evaluation. Various authors have tried to develop a formal method to measure the level of information security at an enterprise wide level (see Chakraborty et al., 2012; Krautsevich et al., 2010; Harrison et al., 1976; Sandhu, 1993).

Abbas et al. (2010) have tried to study three major problems associated with the uncertainty in information security management in various organizations. These three problems are dynamically changing security requirements; the externalities which are caused by a security system; and the outdated assessment of security concerns. The authors have used a framework based on real options valuation for the current study. The authors have shown that real options theory can be used as a coherent methodology in evaluation of challenges related to information security at the organizational level. Their findings can have important implications for information security management at different organizations that are operating in a dynamic environment.

Various authors have also suggested that reusing the login credential – using the same combination of login id and passwords for multiple accounts – can cause serious security issues (see Gaw and Felten, 2006; Zhang et al., 2009; Ives et al., 2004; Bang et al., 2012). One possible reason for this reuse behavior is provided by the cognitive psychology theory. The theory says that human beings have limited memory and retention power and hence have a tendency to reuse the id and password (Miller, 1994). Schneier (2000) has argued that users of information system resources are currently considered as the weakest link in the security chain.

Leach (2003) has argued that internal security threats are currently considered more pressing issue than external security threats, by several organizations. Bang et al. (2012) have argued that due to their limited memory capacity, many internet users reuse their login credentials. These credentials may be any combination of a user ID and passwords. This can cause significant security issues. Therefore the authors have studied the weakness of login credentials. Based on a data set of Internet user the authors have analyzed their behavioral characteristics in terms of their use of login credentials. The authors have found that many internet users use the same login credentials for more than one account. Furthermore, the authors also found that the users' usage patterns are also skewed. The authors have further used this information to develop a vulnerability measure of internet users and have analyzed their current vulnerability to internet malpractices.

Geer et al. (2003) have stressed upon the need for a proper measurement of the information security systems. The authors have also concluded that the information security measurement is inevitable for sustainability of any organization. Fowler (2001) has argued that any form of measurement should communicate some meaning to those who are responsible for measuring. The author has also said that the ones responsible for measurement should aptly understand the meaning conveyed by the measured results.

Smith et al. (2010) have argued that organizations should protect information assets from various crimes associated with cyber usage. These include crimes like web hackers, data breaches, credit card fraud, and identity fraud etc. The authors have investigated information security systems (ISS) within the government while ISS standards are adopted and accredited. The authors found that a strategy which is based on organization size is very vital in motivating and helping organizations to opt for accreditation. Pathari and Sonar (2013) have argued that measuring the information security assurance (ISA) can be a very challenging task. Keeping this fact in mind the authors have tried to develop a framework, which can be helpful in categorizing security requirements into various controls so that their effectiveness can be easily measured. The authors have also proposed an aggregation method which can combine various measures so that a particular indicator reflecting the entire information security assurance can be developed. The authors have further argued that the identified control measures can aid security experts in ensuring their right implementation. This can also assist in finding out the impact of a single control measure on the overall security system.

Kayworth and Whitten (2010) have argued that it is not clear how organizations can become more strategic towards their approach to managing information security. In order to address this concern the authors have interviewed 21 information security employees working in 11 organizations. The authors found that an information security system that is highly strategically focused contains both IT products as well as organizational and social integration mechanism. The authors have further argued that collectively these components form a framework of social and technical approach to information security. According to the authors this framework can help achieve organization three objectives. These include balancing need to protect the information resources against the need to be more productive, managing compliance issues and finally ensuring a proper cultural fit.

Johnston and Hale (2009) have argued that in the current era where businesses are hyper-connected, the organizations are under constant attack from various sources. The authors have empirically examined the information security planning at various stages including the strategic level. The authors have also tried to assess the value enhancing ability of information security programs. The authors found that information security governance is very vital for a Successful information security planning. The authors also concluded that information security is more beneficial to firms which address this concern as an overall enterprise issue. The organizations also gain who integrate information security with the executive planning and strategy formulation.

2.5 Impact Of Information Security Breaches

There have been several studies which indicate of a reported or probable security breaches in various organizations (see Barrows and Clayton, 1996; Saltzer and Schroeder, 1995; Dhillon and Torkzadeh, 2006; Rothstein, 2007). Various studies have examined the reaction of stock markets to the information security initiatives' disclosures by firms (see Gordon et al., 2010; Ito et al., 2010; Campbell et al., 2003).

Privacy as well as the security of electronic health records can be gravely threatened by outside agents such as viruses, worms and hackers. Recent years have witnessed an increasing number of thefts of sensitive medical records (Rothstein, 2007). Various authors have studied the breaches made in the information security systems. These breaches include malicious behavior comprising of acts such as sharing of user ID and passwords, not remembering to take back-ups of important files, leaving the computers unattended and sharing confidential information with other parties (see Leach, 2003; Stanton et al., 2005).

Gerber et al. (2001) have argued that if the information security is inadequate then it may lead to severe consequences. These consequences include damage due to internal errors, invasion of information systems by external agents, breach of confidential data, and systematic internal violation. Townsend and Bennett, (2003) have argued that information security threats and breaches can have severe detrimental effects on organizations. This can include damaging consequences like law suits, loss of clients and even bankruptcy.

Campbell et al. (2003) have argued that the stock price of a company reporting a breach in information security is likely to fall more if the breach leaked important and private information. Conner and Coviello (2004) have argued that information security is slowly but steadily coming into the mainstream. They have also found that information security is currently projected as an integral part of the overall operations rather than just a by-product. Brancheau et al. (1996) have argued that ensuring information system security is rapidly becoming one of most important priority in many companies.

Cavusoglu et al. (2009) have argued that in order to reduce information security risk it is not sufficient to just rely on the technology based solutions. Veltsos et al. (2012) have provided a qualitative descriptive analysis of thirteen notifications regarding data security breach issued by state and federal agencies. They found that most of these notifications typically advise for negative messages. The authors also found that the templates from the state and federal agencies do contain direct patterns that can be effective in informing the users regarding the requirements of law. Thus they consider the templates to be very useful in helping the users to overcome their rational ignorance.

Hoffer and Straub (1989) have done a survey on systems professionals as well as managers of various US firms. The authors found that almost twenty percent of organizations have experienced security breaches in a time span of three years. The authors also suggest that the actual number can be much high since most of these breaches are undetected or are not reported due to fear of negative publicity. Bjorck (2004) has argued that neo-institutional theory should be used in order to study the IT security issues faced by any organization. The author further states that the theory can also be used to elucidate the difference between formal systems of information security and their actual behavior.

2.6 Investment In Information Security And Firm Performance

The final issue concerned with security of medical data is the economic gains arising out of it. Several authors have tried to find out if securing data of employees helps the organization in the long run (see Blakley et al., 2001; Bashir and Christin, 2008; Tashi and Ghernaouti 2008; Blakley, 2002). Many authors have studied the successful implementation of information technology in various organizations (see Franz and Robey 1984; Alavi and Henderson 1981; Markus 1983). While others have focused on developing information systems that possess efficiency, effectiveness and resilience (see Mumford and Weir, 1979; Bostrom and Heinen, 1977).

Weill and Ross (2004) have found that corporations in the US spend around 50 percent of their total capex and around 4.2 percent of their total annual revenues for Information Technology up gradations. Bharadwaj et al. (1999) have argued that a majority of empirical studies that try to find the value created by information technology have considered it as a single and uniform set of assets. On the other hand Brynjolffson and Hitt (1995) have argued that the total investment done in IT should be divided into capital and labor stock.

Floyd and Wooldridge (1990) have argued that the investments made in IT resources reflect the strategy of a firm and also affects its performance. Strassmann (1985) has found that there is no direct relationship between investment in IT and performance as measured by return on investments. Dudley and Lasserre (1989) have found that investments in IT have an indirect effect on performance by reducing the need to store extra inventories.

Barua, Kriebel and Mukhopadhyay (1995) have tried to find the impact of IT investment on firm specific variables like capacity utilization, new product introduction, relative price and inventory turnover quality. The authors found that though investments in IT positively impact some of the intermediate measures of performance, the overall effect is quite low and is insignificant in several cases. Diowert and Smith (1994) have used quarterly data spread over six quarters to find out the impact of IT on variables such as growth rate, inventory levels, and inventory holding costs. The authors found that investments in IT have a positive and significant impact on profitability of various firms. They also found that IT investments result in large productivity benefits.

Hitt and Brynjolfsson (1995) have argued that IT investments result in productivity gains and higher consumer surplus. The authors however found that IT investment does not lead to higher profitability. Prasad and Harker (1997) have found that additional capital investment made to information systems may not lead to higher benefits for the firm. Dewan and Min (1997) have argued that investment in IT acts as a substitute for labor and ordinary capital. Therefore IT investments result in higher productivity and higher returns for the firm. Mukhopadhyay, Rajiv and Srinivasan (1997) have found that there is a positive and significant relationship between investments in IT resources and higher productivity.

Francalanci and Galai (1998) have tried to find out the impact of IT expenditure on employees' composition and overall productivity gains. The authors found that an increase in IT expenses is positively related to productivity gains when it is accompanied by changes made to workers composition. Marwaha and Willmot (2006) have pointed out that IT alignment within an organization helps it in achieving its long term objectives. There have also been studies which have modeled Information security from an economic perspective. These authors have tried to understand the economic or financial risk arising out of any breach or attack on the information security.

Aral and Weill (2007) have tried to find out the relationship between IT investment and firm performance. The authors have developed a model consisting of IT resources which they define as a combination of IT assets and firm capabilities. The authors have argued that IT investments are driven by the strategies of a firm. The authors have also empirically tested their model on 147 US firms for a four year period i.e. from 1999 till 2002. The authors found that there is no relationship between total investment in IT and firm performance. The authors however found a significant relationship between investments made in specific IT assets and performance.

Devraj and Kohli (2003) have tried to study the relationship between investment made in IT and its impact on overall organizational performance. They have based their study on a longitudinal design in which they have collected healthcare data from eight hospitals. They collected monthly data on IT usage and other financial measures. The authors found that it is not the investment in IT resources but its actual usage that affects performance. Thus they have concluded that in order to improve performance organizations must focus on IT usage rather than on IT investments.

Tanriverdi (2006) have argued that unlike other technologies that have limited applicability, information technologies (IT) has wider applicability across different industries. Therefore firms operating in many industries can exploit cross-unit IT synergies. The authors have examined the sources of these synergies for firms having multi-business operations. They have based their study on a sample of 356 Fortune 100 firms that have operations in many businesses. The authors found that as the firms become more and more diversified, the performance gains of IT synergies also increase. They also found that the governance system of IT does not impact the synergies derived out of implementing IT in cross-unit businesses.

Yildirim et al. (2011) have tried to study the organizational information security in SMEs operating in Turkey. The authors have also compared the results obtained with similar information obtained from other countries. The authors carried out their work by floating questionnaires which consisted of 49 questions that were categorized into 9 sections. The questionnaires were sent to 97 SMEs operating in Turkey. The authors found that improvements in security of communications and operations management have a direct and positive impact on various other security parameters as well. These other security parameters consist of personnel, organizational, and physical environment. In addition to this the authors also found that as compared to companies from other countries, Turkish companies do not give that much importance to their IT system's security.

Tarride et al. (2011) have studied the performance of a health care program offered to the Canadian public service employees. The author found that the workplace intervention for healthcare is feasible, is valued by the employees and is also sustainable in the long run. The authors have concluded that workplace intervention for healthcare can prove to be a new framework for assessing and correcting health related issues faced by various employees.

Many studies in the area of information systems have also recognized the IT assets as a medium of creating cross-unit synergy in businesses having many units (see, Sambamurthy and Zmud, 1999; Brown and Magill, 1998). Huang et al. (2014) have applied various economic decision tools in order to model the Healthcare Information Exchanges (HIEs). The authors have modeled HIEs on the basis on their network properties. The authors have aimed to propose valuable insights related to the issue of finding out the optimal investment level in the information security. The authors found out that for various organizations in HIEs, it makes sense to invest in protecting the security events that carry a potential loss which may surpass a critical value. This can help organizations in reducing their overall investment on protection measures. Brynjolfsson and Yang (1997) have argued that the relationship between different measures of firm performance and investments in IT is moderated by organizational capabilities. The authors have also found that if the IT resources are not properly defined then it may lead to derivation of absurd results.

The current has provided the relevant literature related to the topic by investigating various vital aspects of medical data management. Privacy as well as security concerns are extremely critical in medical data handling since employees may confront serious problems if certain sensitive information is leaked to unauthorized parties. In this section we have reviewed and identified the most important security and privacy aspects related to the medical records of employees. We have also classified the themes into six major categories based on similarities and relevance of these themes. The systematic review of literature has enabled us to find out the major gaps existing in the current literature.

3. OBJECTIVE OF THE STUDY

Risk management is a complex process which involves co-ordination at various levels (Chapman and Ward 1996). Managing risk is increasingly becoming the most vital strategic decisions for many firms (Cooper, 2000; Raj, 2013; Zhao et al., 2013). Stakeholders are becoming increasingly concerned about various risks and their impact on the performance and sustainability of firms (Schwarzkopf, 2006; Hartono, 2013; Goodpaster, 1991; Mitchell et al., 1997). An enterprise-wide approach to risk management enables an organization to consider the potential impact of various types of risks related to processes, activities, stakeholders, products and services (Summer, 2000; Liebenberg and Hoyt, 2003; Lam, 2000; Simkins and Ramirez, 2007; Aagedal et al., 2002). One such risk is the risk arising due to breach of information security. This may lead to financial as well as reputational loss for an organization (Huang et al., 2014; Townsend and Bennett, 2003; Cremonini and Nizovtsev, 2010; Ash et al, 2004; Longstaff et al., 2000).

Many people (Huang et al., 2014, Blakley et al., 2001; Bashir and Christin, 2008; Tashi and Ghernaouti 2008; Blakley, 2002) consider health information to be the most confidential type of personal data. Therefore organizations should take utmost care while handling such data. The purpose of the study is to find out the major factors impacting medical data security in the Indian organizations.

4. METHODOLOGY

For the quantitative study a survey has been conducted with the help of a close ended questionnaire. The questionnaire was circulated in the physical mode. Convenience sampling was deployed in order to select the respondents. The validity of the constructs was assessed by means of factor analysis.

4.1 Sample And Data Collection

Employees working in various companies across three industries – Healthcare, IT, and Telecom – were selected to collect responses. These respondents were either in the operations department or in the management department. The target sample size was three hundred (300) respondents. The aim was to have at least 100 respondents from all the three industry segments. Around five hundred (500) respondents were contacted to get the questionnaire filled. The final usable sample consisted of 370 respondents out of which 128 respondents were from the Healthcare industry, 126 were from the IT industry, and 118 were from the Telecom industry.

The rationale for considering these three industries is that they are the upcoming sectors in the Indian economy. The healthcare sector is growing due to changing lifestyles and increased spending on health facilities by Indians. The Indian IT sector mostly consists of export oriented businesses. Low cost advantage and superior skills make India host for various IT related outsourcing activities. The telecom sector in India is growing due to increased mobile penetration in urban and rural areas. The sector mainly consists of voice and data transfer activities.

4.2 Factor Analysis

Factor analysis is a data reduction technique. In this analysis we try to reduce the

independent variables into a few factors. The factors are created in such a way that there is no correlation among them. Thus, factor analysis as a multivariate technique is used to explain variability among the measure and related variables in terms of lower numbers of variables which are generally referred as constructs or factors. This reduces the problem of multicollinearity and also helps in better comprehension of the given data which can be bulky at times. Several authors have applied factor analysis for different purposes (see Prather et al., 1997; Wei et al., 2008; Ferrari, 1992; Preacher and MacCallum, 2002; Baumgartner and Steenkamp, 1996; Richins and Dawson, 1992; Thomson et al., 2005).

The factor analysis is carried out using the principal component analysis (PCA) method. PCA is a statistical technique which applies orthogonal transformation to change a set of related variables into a smaller set consisting of uncorrelated variables. These uncorrelated variables created are generally called as principal components. The number of principal components derived from the PCA is generally less than the number of variables in the original set of data. The transformation is carried out in such a manner that the first component is able to derive the highest variability contained in the initial data. The second component is derived in such a way that it has the highest variability but with the restriction that it is not correlated with the first components.

4.2.1 Conditions:

Before conducting factor analysis, three conditions are required to be met.

- The number of observations should be at least 5 times the number of variables.
- The KMO value should be above 0.5.
- The Bartlett's test should be significant.

Table 1: KMO And Bartlett's Test[2]

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.78
Bartlett's Test of Sphericity	Approx. Chi-Square	9,086.0
	df	190
	Sig.	0.00

Table 1 shows the results of KMO statistics as well as the Bartlett's test. As is evident from the table, the KMO value is above 0.5 and the Bartlett's test is also significant at the 1% level. Thus the data is conducive for factor analysis and we can proceed with further analysis. Also the condition of the total number of observations being at least 5 times the number of variables is comfortably satisfied.

Table 2: Total Variance Explained[3]

Component	**Initial Eigenvalues**			**Extraction Sums of Squared Loadings**			**Rotation Sums of Squared Loadings**		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.4	31.9	31.9	6.4	31.9	31.9	4.6	23.2	23.2
2	5.1	25.6	57.5	5.1	25.6	57.5	4.4	21.9	45.1
3	3.7	18.3	75.8	3.7	18.3	75.8	4.4	21.9	67.0
4	2.2	11.0	86.8	2.2	11.0	86.8	4.0	19.8	86.8
5	0.6	2.9	89.6						
6	0.4	1.8	91.4						
7	0.3	1.5	92.9						
8	0.3	1.3	94.2						
9	0.2	1.1	95.2						
10	0.2	1.0	96.2						
11	0.2	0.8	97.0						
12	0.1	0.6	97.6						
13	0.1	0.5	98.1						
14	0.1	0.4	98.6						
15	0.1	0.3	98.9						
16	0.1	0.3	99.2						
17	0.1	0.3	99.5						
18	0.0	0.2	99.7						
19	0.0	0.2	99.9						
20	0.0	0.1	100.0						

[2] Source: This table has been created by the author. Software package SPSS has been used for performing statistical analyses.

[3] Source: This table has been created by the author. Software package SPSS has been used for performing statistical analyses.

The above table displays the results of total variance explained. The table also shows the Eigenvalues of the factors. Since we have selected the criteria of eigen value greater than one, the second panel of the table shows the eigen values and the variance explained of only those factors which have eigen values of greater than one. As is clear from the table, we should go for a four factor solution. The four factors together explain around 86% of the total variance of the original data. Thus we have obtained a very good explanatory model.

Table 3: Rotated Component Matrix[4]

	Component			
	1	2	3	4
My organization has a well defined Policy on medical data protection	0.96			
The medical data protection policy in my organization is adequately resourced	0.95			
The medical data protection policy in my organization is supported by management infrastructure	0.94			
The policy on medical data protection in my organization is reviewed regularly.	0.94			
There are no major practical or technical difficulties in providing the medical data	0.90			
Employees in my organization are made aware, before they provide medical data, of why this data is being collected		0.94		
There is an identifiable person responsible for medical data protection in my organization		0.92		
In my organization staff is trained in the necessary security controls and procedures for medical data handling		0.91		
All individuals who are authorized to process medical data in my organization receive appropriate training		0.90		
In my organization there are procedures that allow employees to access medical data which relate to them		0.90		
My organization retains all the proofs of lawful processing of medical data			0.95	
In my organization the changes to software or processing environment are considered in the context of medical data protection obligations			0.93	
My organization has the full extent of medical data processing authorized by law and regulations			0.93	
In my organization medical data protection considerations are taken into account during the development and purchase of hardware and software			0.89	
In my organization processes are in place for documenting and reviewing all identified quality issues related to medical data			0.84	
There are security controls and procedures in my organization which ensure the integrity of the medical data				0.93
The security controls and procedures in my organization for ensuring the integrity of the medical data are effective				0.91
My organization has formal criteria for deletion of medical data				0.89
My organization checks whether the medical data provided by employees is up to date				0.88
My organization checks the medical data provided by employees for its adequacy				0.76

[4] Source: This table has been created by the author. Software package SPSS has been used for performing statistical analyses.

Table 3 shows the rotated component matrix and the corresponding loadings. The loading are arranged in descending order and the loadings below 0.4 have been hidden. The rotated component analysis gives a much better solution. As is evident from the table that there are no cross loadings. Also we have obtained a four factor solution. All the factor loadings are above 0.75. Thus we can conclude that the factor solution obtained is appropriate. There are five variables loading into each factor. The highest factor loading is of 0.96 and the lowest factor loading is of 0.76. All other loading lie between these two scores. Most of the loadings are in the range of 0.9 to 0.95. Thus the loadings obtained are appropriate and the factor structure is proper.

The **first factor** has five variables loaded into it namely “my organization has a well defined Policy on medical data protection”, “the medical data protection policy in my organization is adequately resourced”, “the medical data protection policy in my organization is supported by management infrastructure”, “the policy on medical data protection in my organization is reviewed regularly” and, “there are no major practical or technical difficulties in providing the medical data”. This factor basically points at the policies related to the medical data security. The factor also talks about the organizational resources supporting the security of medical data. Thus we can name the as factor as to “**Policy and Resources**” aspect of medical data.

The **second factor** has five variables loaded into it namely “employees in my organization are made aware, before they provide medical data, of why this data is being collected”, “there is an identifiable person responsible for medical data protection in my organization”, “in my organization staff is trained in the necessary security controls and procedures for medical data handling”, “all individuals who are authorized to process medical data in my organization receive appropriate training”, and, “in my organization there are procedures that allow employees to access medical data which relate to them”. This factor mostly talks about various trainings and employees awareness programs. Thus we can name the as factor as to “**Training and Employee Awareness**” aspect of medical data.

The **third factor** has five variables loaded into it namely “my organization retains all the proofs of lawful processing of medical data”, “in my organization the changes to software or processing environment are considered in the context of medical data protection obligations”, “my organization has the full extent of medical data processing authorized by law and regulations”, “in my organization medical data protection considerations are taken into account during the development and purchase of hardware and software”, and “In my organization processes are in place for documenting and reviewing all identified quality issues related to medical data”. This factor mainly explains the legal considerations and the standards which are required to be met by companies. Thus we can name the as factor as to “**Standards and Regulations**” aspect of medical data.

The **fourth factor** has five variables loaded into it namely “there are security controls and procedures in my organization which ensure the integrity of the medical data”, “the security controls and procedures in my organization for ensuring the integrity of the medical data are effective”, “my organization has formal criteria for deletion of medical data”, “my organization checks whether the medical data provided by employees is up to date”, and, “my organization checks the medical data provided by employees for its adequacy”. This factor mainly talks about various controls that need to be applied in order to secure the medical data. Thus we can name the as factor as to “**Processes and Controls**” aspect of medical data. Table 4 presents a summary of the factors obtained and their naming.

Table 4: Factor Naming[5]

No.	Statement	Name of Factor
4.03	My organization has a well defined Policy on medical data protection;	**Policy and Resources**
4.13	The medical data protection policy in my organization is adequately resourced;	
4.16	The medical data protection policy in my organization is supported by management infrastructure;	
4.09	The policy on medical data protection in my organization is reviewed regularly;	
4.17	There are no major practical or technical difficulties in providing the medical data	
4.19	Employees in my organization are made aware, before they provide medical data, of why this data is being collected;	**Training and Employee Awareness**
4.08	There is an identifiable person responsible for medical data protection in my organization;	
4.02	In my organization staff is trained in the necessary security controls and procedures for medical data handling;	
4.11	All individuals who are authorized to process medical data in my organization receive appropriate training;	
4.20	In my organization there are procedures that allow employees to access medical data which relate to them	
4.15	My organization retains all the proofs of lawful processing of medical data;	**Standards and Regulations**
4.18	In my organization the changes to software or processing environment are considered in the context of medical data protection obligations;	
4.10	My organization has the full extent of medical data processing authorized by law and regulations;	
4.04	In my organization medical data protection considerations are taken into account during the development and purchase of hardware and software;	
4.06	In my organization processes are in place for documenting and reviewing all identified quality issues related to medical data	
4.01	There are security controls and procedures in my organization which ensure the integrity of the medical data;	**Processes and Controls**
4.07	The security controls and procedures in my organization for ensuring the integrity of the medical data are effective;	
4.14	My organization has formal criteria for deletion of medical data;	
4.05	My organization checks whether the medical data provided by employees is up to date;	
4.12	My organization checks the medical data provided by employees for its adequacy	

Source: This table has been created by the author. Software package SPSS has been used for performing statistical analyses.

5. THEORRTICAL MODEL FOR ACCESSING SECURITY OF MEDICAL DATA

Based on the results, Security of medical data assessment model can be made. Figure 1 proposes such a model. The results suggest some support for the basic structure of this model. The factor analysis clearly revealed six dimensions of security.

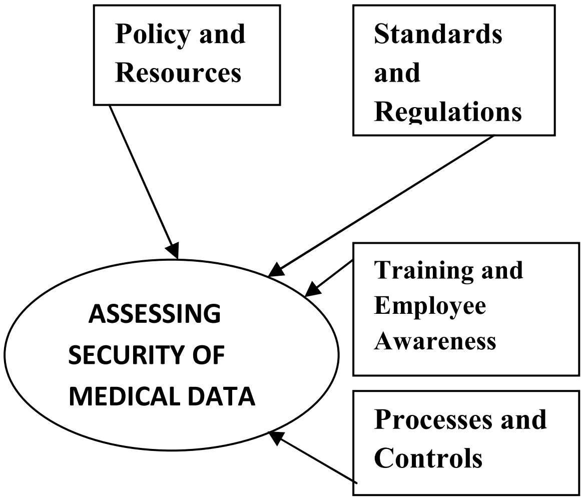
Policy and Resources
Standards and Regulations
Training and Employee Awareness
Processes and Controls
ASSESSING SECURITY OF MEDICAL DATA

Figure 2: A Conceptual Model Of Medical Data Security Assessment

6. CONCLUSION

The study has two major contributions. First, the study found evidence that medical data management is a complicated matter and consists of several dimensions. The study identified four key dimensions for Indian organizations. Second, the study also highlighted that there are multiple constructs that should be considered while measuring the overall information security within an organization. These constructs or factors should be evaluated both individually as well as collectively in order to make the information secure and reliable.

6.1 Implication For The Management

The major implication of the current study is that managers should look into IT as an enabling factor in protecting the overall organizational data in general and medical data in particular. The managers should specifically focus on four aspects of medical data namely, controls, employees and training, policies, and regulations. These four factors should be viewed as four pillars that are supporting the overall data security within an organization. The appraisals of IT managers can also be linked to their performance in terms of these four factors. Further, all the key personnel, irrespective of their departments, should be made aware of these four factors. This will ensure the considerations of these four factors in all the major decisions made by the organization.

The major limitation of the study is that it is confined to only three sectors namely Healthcare, Telecom & IT. Further we have studied only one country i.e. India.

7. SCOPE OF FUTURE RESEARCH

One of the most important aspects of information security is its impact on other related organizations. These organizations include subsidiaries, partners, customers, and competitors. There can be several positive as well as negative spillovers of information security practices to these related organizations. The impact and nature of such spillovers is an open question. This can be studied in detail in order to provide more depth and breadth to the topic of information security.

REFENCES:

[1] Greenhalgh, T., Hinder, S., Stramer, K., Bratan, T., & Russell, J. (2010). Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace. BMJ: British Medical Journal, p341.

[2] Allison, G. T. (1971). Essence of decision. Boston: Little, Brown, p536.

[3] Yin, R. K. (1981). The case study crisis: some answers. Administrative science quarterly, 26(1), p58-65.

[4] Eisenhardt, K. M. (1989). Building theories from case study research. Academy of management review, 14(4), p532-550.

[5] Neubauer, T., & Heurix, J. (2011). A methodology for the pseudonymization of medical data. International journal of medical informatics, 80(3), p190-204.

[6] Kahn, S., & Sheshadri, V. (2008). Medical record privacy and security in a digital environment. IT professional, 10(2), 46-52.

[7] Elger, B. S., Iavindrasana, J., Lo Iacono, L., Müller, H., Roduit, N., Summers, P., & Wright, J. (2010). Strategies for health data exchange for secondary, cross-institutional clinical research. Computer methods and programs in biomedicine, 99(3), p230-251.

[8] Management, 10(4). Reis, F. F., Costa-Pereira, A., & Correia, M. E. (2008). Access and privacy rights using web security standards to increase patient empowerment. Studies in health technology and informatics, 137, 275-285.

[9] Hembroff, G. C., & Muftic, S. (2010). SAMSON: Secure access for medical smart cards over networks. In World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a (pp. 1-6). IEEE.

[10] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation.International Journal of Accounting Information Systems, 13(3), p228-243.

[11] Cox, A., Connolly, S., & Currall, J. (2001). Raising information security awareness in the academic setting. Vine, 31(2), p11-16.

[12] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS quarterly, 34(3).

[13] Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS quarterly, 34(3), p503-522.

[14] D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, 20(1), p79-98.

[15] Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management, 29(6), p449-457.

[16] Lemaire, E. D., Deforge, D., Marshall, S., & Curran, D. (2006). A secure web-based approach for accessing transitional health information for people with traumatic brain injury. Computer methods and programs in biomedicine, 81(3), p213-219.

[17] Ruotsalainen, P. (2004). A cross-platform model for secure Electronic Health Record communication. International Journal of Medical Informatics, 73(3), p291-295

[18] Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements and solutions in electronic health records: lessons learned from a comparative study. Journal of medical systems, 34(4), p629-642.

[19] Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. International journal of medical informatics, 80(2), e26-e31.

[20] Kraemer, K. L., & King, J. L. (1988). Computer-based systems for cooperative work and group decision making. ACM Computing Surveys (CSUR), 20(2), p115-146.

[21] Sproull, L., & Kiesler, S. (1986). Reducing social context cues: Electronic mail in organizational communication. Management science, 32(11), p1492-1512.

[22] Gerber, M., von Solms, R., & Overbeek, P. (2001). Formalizing information security requirements. Information Management & Computer Security, 9(1), p32-37.

[23] Rudolph, K., Warshawsky, G., & Numkin, L. (2002). Security awareness.Computer Security Handbook, p29-1.

[24] Jafari, S., Mtenzi, F., Fitzpatrick, R., & O'Shea, B. (2010). Security metrics for e-healthcare information systems: a domain specific metrics approach. Int. Journal of Digital Society, 1(4), p238-245.

[25] Foltz, C. B., Schwager, P. H., & Anderson, J. E. (2008). Why users (fail to) read computer usage policies. Industrial Management & Data Systems, 108(6), 701-712.

[26] Bouhaddou, O., Cromwell, T., Davis, M., Maulden, S., Hsing, N., Carlson, D., & Fischetti, L. (2012). Translating standards into practice: Experience and lessons learned at the Department of Veterans Affairs. Journal of biomedical informatics, 45(4), p813-823.

[27] Culnan, M. J., Foxman, E. R., & Ray, A. W. (2008). Why IT executives should help employees secure their home computers. MIS Quarterly Executive, 7(1), p49-56.

[28] Scott, M. D. (1997). Liability in cyberspace—III: Creating a corporate internet acceptable use

policy. Computer Law & Security Review, 13(6), p451-453.

[29] Murray, B. (1991). Running corporate and national security awareness programmes. In Proceedings of the IFIP TC11 Seventh International Conference on IS security p203-207.

[30] Peltier, T. (2000). How to build a comprehensive security awareness program. COMPUT SECUR J, 16(2), p23-32.

[31] Hadland, T. (1998). IS Security Management: An Awareness Campaign. In Proceedings of New Networks, Old Information: UKOLUG98, UKOLUG's 20th Birthday Conference.

[32] Kajava, J., & Siponen, M. T. (1997). Effectively Implemented IS security Awareness-An Example from University Environment. In Proceedings of IFIP-TC (Vol. 11, pp. 105-114).

[33] Wood, C. C. (2002). The human firewall manifesto. Computer Security Journal, 18(1), 15-18.

[34] Lafleur, L. M. (1992). Training as part of a security awareness program. Computer Control Quarterly, 10(4), 4-11.

[35] Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy.

[36] Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 34(3), 487.

[37] Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), p2799-2816.

[38] Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS quarterly, 34(3).

[39] LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. Communications of the ACM, 51(3), p71-76.

[40] Gowen III, C. R., McFadden, K. L., & Tallon, W. J. (2006). On the centrality of strategic human resource management for healthcare quality results and competitive advantage. Journal of management development, 25(8), p806-826.

[41] Bartol, N., Bates, B., Goertzel, K.M. and Winograd, T. (2009). Measuring Cyber Security and Information Assurance (State-of-the-Art Report (SOAR)). Information Assurance Technology Analysis Center (IATAC), Herndon, VA.

[42] Chakraborty, A., Sengupta, A., & Mazumdar, C. (2012). A formal approach to information security metrics. In Emerging Applications of Information Technology (EAIT), 2012 Third International Conference on (pp. 439-442). IEEE.

[43] Krautsevich, L., Martinelli, F., & Yautsiukhin, A. (2010, August). Formal approach to security metrics.: what does more secure mean for you?. In Proceedings of the Fourth European Conference on Software Architecture: Companion Volume (pp. 162-169). ACM.

[44] Harrison, M. A., Ruzzo, W. L., & Ullman, J. D. (1976). Protection in operating systems. Communications of the ACM, 19(8), p461-471.

[45] Sandhu, R. S. (1993). Lattice-based access control models. Computer, 26(11), p9-19.

[46] Abbas, H., Magnusson, C., Yngstrom, L., & Hemani, A. (2011). Addressing dynamic issues in information security management. Information Management & Computer Security, 19(1), p5-24.

[47] Gaw, S., & Felten, E. W. (2006, July). Password management strategies for online accounts. In Proceedings of the second symposium on Usable privacy and security (pp. 44-55). ACM.

[48] Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). Improving multiple-password recall: an empirical study. European Journal of Information Systems,18(2), p165-176.

[49] Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. Communications of the ACM, 47(4), p75-78.

[50] Bang, Y., Lee, D. J., Bae, Y. S., & Ahn, J. H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. International Journal of Information Management, 32(5), p409-418.

[51] Miller, G. A. (1994). The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological review, 101(2), p343.

[52] Schneier, B. (2011). Secrets and lies: digital security in a networked world. John Wiley & Sons.

[53] Leach, J. (2003). Improving user security behaviour. Computers & Security,22(8), 685-692.

[54] Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organization. MIS quarterly, 34(3), p463-486.

[55] Pathari, V., & Sonar, R. M. (2013). Deriving an information security assurance indicator at the organizational level. Information Management & Computer Security, 21(5), p401-419.

[56] Barrows, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. Journal of the American Medical Informatics Association, 3(2), p139-148.

[57] Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(9), p1278-1308.

[58] Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), p293-314.

[59] Rothstein, M. A. (2007). Health privacy in the electronic age. The Journal of legal medicine, 28(4), p487-501.

[60] Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. MIS quarterly, 34(3).

[61] Ito, K., Kagaya, T., & Kim, H. (2010). Information security governance to enhance corporate value. NRI Secure Technologies.

[62] Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11(3), p431-448.

[63] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), p124-133.

[64] Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2009). Information security control resources in organizations: A multidimensional view and their key drivers. working paper, Sauder School of Business, University of British Columbia.

[65] Veltsos, J. R. (2012). An Analysis of Data Breach Notifications as Negative News. Business Communication Quarterly, 75(2), p192-207.

[66] Blakley, B. (2002). The measure of information security is dollars. In Workshop of Economics and Information Security.

[67] Bashir, M., & Christin, N. (2008). Three case studies in quantitative information risk analysis. In Proceedings of the CERT/SEI Making the Business Case for Software Assurance Workshop (pp. 77-86).

[68] Tashi, I., & Ghernaouti-Helie, S. (2008, June). Efficient security measurements and metrics for risk assessment. In Internet Monitoring and Protection, 2008. ICIMP'08. The Third International Conference on (pp. 131-138). IEEE.

[69] Franz, C. R., & Robey, D. (1984). An investigation of user-led system design: rational and political perspectives. Communications of the ACM, 27(12), p1202-1209.

[70] Alavi, M., & Henderson, J. C. (1981). An evolutionary strategy for implementing a decision support system. Management Science, 27(11), p1309-1323.

[71] Markus, M. L. (1983). Power, politics, and MIS implementation. Communications of the ACM, 26(6), p430-444.

[72] Mumford, E., & Weir, M. (1979). Computer systems in work design--the ETHICS method: effective technical and human implementation of computer systems: a work design exercise book for individuals and groups. Wiley.

[73] Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective PART I: THE CAUSES. MIS quarterly, 1(3).

[74] Barua, A., Kriebel, C. H., & Mukhopadhyay, T. (1995). Information technologies and business value: An analytic and empirical investigation. Information systems research, 6(1), p3-23.

[75] Brynjolfsson, E., & Hitt, L. (1995). Information technology as a factor of production: The role of differences among firms. Economics of Innovation and New technology, 3(3-4), p183-200.

[76] Prasad, B., & Harker, P. T. (1997). Examining the contribution of information technology toward productivity and profitability in US retail banking. The Wharton Financial Institutions Center Working Papers, 97(9).

[77] Dewan, S., & Min, C. K. (1997). The substitution of information technology for other factors of production: A firm level analysis. Management Science, 43(12), p1660-1675.

[78] Mukhopadhyay, T., Rajiv, S., & Srinivasan, K. (1997). Information technology impact on process output and quality. Management Science, 43(12), p1645-1659.

[79] Francalanci, C., & Galal, H. (1998). Information Technology and Worker Composition: Determinants of Productivity in the Life Insurance Industry. MIS Quarterly, 22(2).

[80] Marwaha, S., & Willmott, P. (2006). Managing for scale, speed, and innovation. McKinsey Quarterly, 4, 87.

[81] Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance: How resource allocations and

organizational differences explain performance variation. Organization Science, 18(5), p763-780.

[82] Devaraj, S., & Kohli, R. (2003). Performance impacts of information technology: is actual usage the missing link?. Management science, 49(3), p273-289.

[83] Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. International Journal of Information Management, 31(4), p360-365.

[84] Sohal, A. S., & Ritter, M. (1995). Manufacturing best practices: observations from study tours to Japan, South Korea, Singapore and Taiwan. Benchmarking for Quality Management & Technology, 2(4), p4-14.

[85] Michell, P., & Palihawadana, D. (2008). Exploring the components of success for the Korean chaebols. Journal of Business & Industrial Marketing, 23(5), p311-322.

[86] Greidanus, N. S., & Märk, S. (2012). An Exploration of Internal Corporate Venturing Goals in Family Firms. Journal of Small Business & Entrepreneurship, 25(2), p169-183.

[87] Cassia, L., De Massis, A., & Pizzurno, E. (2011). An exploratory investigation on NPD in small family businesses from northern Italy. International journal of business, management and social sciences, 2(2), p1-14.

[88] Glaser, B. G. (1992). Emergence vs forcing: Basics of grounded theory analysis. Sociology Press.

[89] Loy, T. C. J. (2010). Dynasting Across Cultures: A Grounded Theory of Malaysian Chinese Family Firms (Doctoral dissertation, UNIVERSITY OF MINNESOTA).

[90] Danes, S. M., Haberman, H. R., & McTavish, D. (2005). Gendered discourse about family business. Family Relations, 54(1), p116-130.

[91] Kansikas, J., & Nemilentsev, M. (2010). Understanding family dynasty: Nurturing the corporate identity across generations. Int. Journal of Business Science and Applied Management, 5(3).

[92] Zachary, M. A., McKenny, A., Short, J. C., & Payne, G. T. (2011). Family Business and Market Orientation Construct Validation and Comparative Analysis. Family Business Review, 24(3), p233-251.

[93] Ritterspach, F., & Bruche, G. (2012). Capability creation and internationalization with business group embeddedness–the case of Tata Motors in passenger cars. European Management Journal, 30(3), p232-247.

[94] Orhan, M., & Scott, D. (2001). Why women enter into entrepreneurship: an explanatory model. Women in Management Review, 16(5), p232-247.

[95] Eisenhardt, K. M. (1989). Building theories from case study research. Academy of management review, 14(4), p532-550.

[96] Tellis, W. (1997). Results of a case study on information technology at a university. The qualitative report, 3(4), 76.

[97] Card, D., & Krueger, A. B. (1993). Minimum wages and employment: A case study of the fast food industry in New Jersey and Pennsylvania (No. w4509). National Bureau of Economic Research.

[98] Dyer, J., & Nobeoka, K. (2002). Creating and managing a high performance knowledge-sharing network: the Toyota case.

[99] Sako, M. (2004). Supplier development at Honda, Nissan and Toyota: comparative case studies of organizational capability enhancement. Industrial and corporate change, 13(2), p281-308.