*Ashish Ukidve, et. al. International Journal of Engineering Research and Applications*
*www.ijera.com*
*ISSN: 2248-9622, Vol. 11, Issue 5, (Series-VI) May 2021, pp. 18-24*

RESEARCH ARTICLE OPEN ACCESS

# Analysis of evolution of information security management practices in organisations providing IT development & IT Enabled services

Ashish Ukidve[1], Dr S S Mantha[2], Dr D N Reddy[3]
*1 Principal, Vidyalankar Polytechnic, Mumbai, India*
*2 Ex-Chairman, AICTE, Chancellor-KL University-AP-522502*
*3 Professor, Osmania University, Former VC , JNTU-Hyderabad-500007*

**ABSTRACT**
With the increasing reliance of businesses over information and information system, it has become crucial for organizations to guard their critical information assets against loss , theft or misuse. With the growth of IT/ICT field and the developments in the ways of information is generated, processed, stored, distributed globally over communication links, the information security landscape has been changing very rapidly. Organizations need to have a balanced mix of technical, management and behavioural aspects to overcome this challenge. This analysis attempts to review the ISM practices followed by ITdevelopment and IT enabled services companies. Observations of this analysis and correlations among various ISM factors may help to develop an organizational ISM framework which can be useful to prioritize various organizational ISM practices.
***Keywords -*** cyber breaches, risk management, security management practices , security policy

---

Date of Submission: 15-05-2021 Date of Acceptance: 31-05-2021

---

## I. INTRODUCTION

With the increasing reliance of businesses over information and information system, it has become crucial for organizations to guard their critical information assets against loss , theft or misuse. While the technical advancements have become enablers for organizations to process business information in a faster, more efficient way, it has also increased the concerns of information security threats and challenges for them. With the growth of IT/ICT field and the developments in the ways of information is generated, processed, stored, distributed globally over communication links, the information security landscape has been changing very rapidly. According to Ernst & Young's (2010) global information security survey, 254 *Global Business Review 20(1, )* in 46 per cent cases companies have indicated that their annual investment in managing the information security have increased (Ernst & Young, 2010). The report also highlights that 60 per cent respondents perceive that use of social networking, cloud computing, smart phones and other personal devices in enterprises have increased the level of risk faced by them (Ernst & Young, 2010). In such a scenario, organizations need to be armed with the technologically advanced solutions. However, technology can address only part of this problem. Information security is a multidimensional discipline (Posthumus & von Solms, 2004; von Solms, 2001) . Von Solms (2001) identifies different dimensions of information security and also explains the interrelationships among them. Physical security, technical security, operational security, mobile security, application security, behavioural security are important considerations of information security. Organizations need to have a balanced mix of technical, management and behavioural aspects to overcome this challenge (Ashenden, 2008; Werlinger, Hawkey & Beznosov, 2009) .

Information security is the 'application of a managerial processes and technical methods on the information resources (hardware and communication infrastructure, software and data) in order to keep organizational assets and personal privacy protected' (Hong, Chi, Chao & Tang, 2006) . Whereas, information security management (ISM) consists the set of activities involved in configuring resources in order to meet information security needs of an organization (Ashenden, 2008) . Since ISM is a collective responsibility of employees in any organization, assessment of ISM activities at various organizational levels (i.e., strategic,

executive and operational) becomes essential (Ma, Schmidth & Pearson, 2009) .

The evolution of ISM discipline, as discussed by von Solms (2000, 2006) , can be considered to have come about in four phases. In the first phase , the "technical phase", various tools and techniques were applied to handle various information security issues in the organization (where the build-in security features, such as user-id, passwords, and access control lists were prevalent - the mainframe era). With the advancements of distributed computing World Wide Web and Internet, organizational boundaries started blurring. This led the evolution of the "management phase", where information security got the attention of the board and senior management (von Solms, 2000) . During this phase organizations started focusing on various management aspects of information security, such as policy (Bulgurcu, Cavusoglu & Benbasat, 2010; Hong et al., 2006) , training programmes (Furnell, Gennatou & Dowland, 2002; Knapp, Marshall, Rainer & Morrow, 2006), top-management support and involvement (Kankanhalli, Teo, Tan & Wei, 2003) among others. Once this has started becoming the standard practice across organizations, third phase, the "institutional phase" emerged. In the third phase, the focus was more on standardization of the best practices of information security. International standards and certifications (e.g., BS 7799 and ISO/IEC 17799) were developed, and the attention was to build an information security culture (Knapp et al., 2006; Thomson, von Solms & Louw, 2006) in organizations. Followed by this, the "governance phase" evolved which emphasized that the organizational ISM is responsibility of corporate governance. The building blocks of the governance phase include information security objectives and strategies, organizational structure, commitment of board and top management, risk management, resource management, regulatory and compliance enforcement (Moulton & Coles, 2003; von Solms, 2006) .

Over a period, with the development of ISM discipline, many frameworks for organizational ISM have been strucutred (e.g., Eloff & Eloff, 2005; ISO/IEC 27002:2005, 2005; Ma et al., 2009; Musa, 2010;

Perks & Beveridge, 2003; Posthumus & von Solms, 2004) . Singh, Gupta and Ojha (2014) have summarized some of these frameworks along with their key identified factors. Some of these factors are external in nature, such as changing security threats, risks, legal/regulatory environment, standards and market situations, whereas business issues, project outsourcing, IT infrastructure, organizational policies and objectives constitute the internal factors (Alexandrova, 2015; Posthumus & von Solms, 2004) .

On similar lines, Werlinger et al. (2009) have categorized various organizational ISM challenges into human, technical and organizational factors. von Solms (2006) discussed various strategic, executive and operational factors building an information security governance model for organizations.

For implementing a robust ISM system , organizations need a balanced mix of these three factors

according to the dynamic business requirements (Kayworth & Whitten, 2010) . Researchers have tried to examine organizational ISM practices in varying contexts. For example, Hong et al. (2006) studied the organizational ISM practices in the context of Taiwan; and Musa (2010) identified various organizational information security governance practices of Saudi organizations.

**Table - 1** below presents some of the organizational ISM case studies carried out by researchers in varied contexts -

| Authors | Perspective | Method adopted | Main Findings |
|---|---|---|---|
| Doughty ( 2003) | Information Security in a Medium size organization | Gap Analysis | Implementation of an enterprise security framework is must |
| Khalfan ( 2004) | IT outsourcing projects of public and private sector organizations in Kuwait | Questionnaire survey and semi-structured interviews | Information security risk outdo other project outsourcing concern like loss of control |
| Zakarta ( 2004) | Information Security culture challenges in a public sector organization in Malaysia | Questionnaire survey and semi-structured interviews, and reviews of InfoSec documents | Research design on security culture – identifying employees' InfoSec behavior |
| Nikhoma ( 2008) | Fin Sector case study – Large Bank | Questionnaire, Interviews | Sec concerns of general management have different |

| | | | |
|---|---|---|---|
| | | | perspective from network security personnel |
| Harnesk ( 2011) | Analyzing security behavior in public nursing centre | Interviews | Discipline and agility play vital role in security behavior |
| Picot, Kranz ( 2013) | ISM practices of Indian and German organizations | Semi Structured Interviews | Ind.type, Org Size, culture and regulatory compliance are key determinants of ISM |
| Parsons, McCormac ( 2014) | Infosec vulnerabilities in 3 Australian govt orgn | Web based Q-nnaire | Key InfoSec awareness concerns include wireless security, social media and reporting of sec incidents |
| Pedron(2016) | Distractions in Security culture after merger | Semi Structured Interviews | Effective communication and defining clear group boundaries are paramount for ISM |

**Source:** Prepared by the authors.

## II. METHODOLOGY

This study examines the ISM practices of IT—services and development organizations in India using interpretive case study approach. Following the qualitative research route, semi structured interviews were conducted to investigate the ISM practices of the companies. To capture multiple viewpoints, interview respondents were selected across the hierarchy in organizations, based on purposive sampling technique. Interviews were conducted, one-to-one in the real-life setting of the respondents. For the interview purpose, a semi-structured questionnaire template was used. The template consists of ISM factors - Top Management Support , Information Security Requirements, , Information Security Policy, Information Security Awareness, Information Security Training, ISM Best Practices , Information Security Culture, Information Security Audit, , Asset Management, Information Security Incident Management, ISM Effectiveness and Information Security Regulations Compliance.

Total 10 interviews were conducted, five from each case organizations and transcripts were prepared for analyzing further. Profiles of the respondents are given in Table below -

**Table 2.** Profile of organisations & interviewed respondents

| | Description of services provided by company and customer profile | Profile of respondent | Experience ( in years) |
|---|---|---|---|
| Case I – Software development company<br><br>Employee base - 60 | - IT consulting, web design and development, mobile applications develop ment, robotics and Internet marketing.<br>- Caters clients from a wide range of industries including aerospace, automotive, consumer goods, food, metal fabrication, medical, pharmaceutical and solar panel, among others. | Managing Director | 20 |
| | | Project coordinator | 10+ |
| | | Team lead—.(dot) Net | 6+ |
| | | Technical associate | 5 |
| | | Network Engineer | 3+ |
| | | | |
| Case II – IT enables service provider company<br><br>Employee base -750 | - Designs, develops, implements and maintains IT systems, products and services of one of the major government institutions in India.<br>- IT solutions, manage overall infor- mation system and give IT consulting services to its parent organization. | Chief InformationSecurity Officer (CISO) and General Manager | 23 |
| | | General manager-IT networks | 25 |
| | | Sr Enginieer – IT Networks | 15 |
| | | Sr Softqare Engineer – Infra & Security | 7 |
| | | IT Engineer | 5 |

The study adopts a two-step methodology for data analysis and presentation. Initially, the observations derived from interviews are presented using descriptive analysis methodology. Creswell (1994) illustrates the descriptive research methodology as, 'it is to gather information about the present condition of a case to describe its situation, and to investigate the cause/s of particular phenomena'. The interview responses were assessed in respect to general and distinctive phenomena that reflect upon points of interest to fulfil the objectives of the study (Babbie, 2004) . That results in a descriptive review of current practices of organizational ISM of the cases under study.

For the next process, SAP-LAP method of inquiry (Sushil, 2000, 2001) was used to systematically analyse the cases based on various Situations, involved Actors and various Processes for organizational ISM functions. The interaction of SAP leads to various LAP activities. Based on the Learning derived from this interplay, various Actions are identified. That leads to the improved Performance of situations, actors and processes (Sushil, 2001) . The analysis brings additional insights and is helpful in identifying the key areas of improvements (Husain, Sushil & Pathak, 2002; Kak, 2004; Singh et al., 2013; Thakkar, Kanda & Deshmukh, 2008).

## III. MAJOR OBSERVATIONS

| Domain of observation | Org | Observations |
|---|---|---|
| Information Security Requirements | I | Any information security breach incident…<br><br>- Affects the productivity<br>- Result into serious outcomes, such as financial losses, loss of productivity, delayed projects, loss of intellectual property, losing clients and, above all, loss of reputation.<br><br>- The top management and software developers acknowledge that information security is the critical aspect for business continuity of the organization. |
| | II | - Information security is essential since customers of the are citizens, any deviation in data/information and information system will result in large public outcry. |
| Top Management Support | I | - Although , awareness is there about the importance of information security for the organization, a consistent support for the same is missing<br>- Budget constraints for ISM<br>- reluctant approach of the senior management towards this issue.<br>- There is no information security officer or any similar authority in the company.<br>- ISM activities of the organization are managed by the network team. This leads to lack of co-ordination and control. |
| | II | - CISO has been appointed in the organization due to which information security has got attention<br>- Two team members are responsible to manage various ISM functions of the organization.<br>- Senior management has realized the importance of information security and is willing to support its various functions<br>- Lack of skilled manpower and funds to support various ISM functions in the organization. |
| Information Security Policy | I | - There is no documented information security policy<br>- The information security roles and responsibilities of employees are not defined.<br>- There is no classification of accountabilities for various information security-related functions in the organization.<br>- Employees take actions on their own In an ad-hoc manner, to manage information security related to their work. |

| | | |
|---|---|---|
| | II | - The organization has officially released a comprehensive information security policy which covers roles and responsibilities of employees, vendors and third-party contractors.<br>- There is a clause in policy to review it annually |
| Information Security Training | I | - There is no formal information security training programmes for employees neither at the time of joining the company nor later. |
| | II | - There are various internal as well as external information security training programmes for employees such as 'general awareness training' for every employee, and 'specific area related training' specific to domain<br>- Every group has a representative that coordinates information security activities of the group. |
| Information Security Awareness | I | - Employees very less aware about various information security threats and counter measures<br>- No communication on information security roles and responsibilities of employees.<br>- General lack of awareness about penalties or legal consequences of any information security breach incident.<br>- There is no advisor to consult/discuss ISM concerns and issues in the organization. |
| | II | - Efforts were taken to communicate possible risks, threats and countermeasures to employees through various training programmes conducted internally as well as outside the organization.<br>- Organization's information security policy and guidelines are published on the Intranet and employees<br>- Employees can raise and discuss ISM-related issues/concerns over internal mail system.<br>- Every employee has to sign a compliance declaration for organization's information security policy.<br>- CERT-In acts as a government appointed advisor for various ISM activities and functions of the organization |
| Information Security Culture | I | - A lacks in terms of creating a culture of ISM in day-to-day activities of employees. In general, employees do not see information security as a part of their job<br>- e, ISM practices, such as changing passwords at regular basis, not to share passwords, take regular backups of critical data, are not been followed by employees and are mostly seen as a burden. There |
| | II | - With the help of regularly conducted information security training and awareness programmes, Case B has an information security culture<br>- There are further plans to start a forum where employees can exchange their ideas and share their concerns with senior officials regarding ISM.<br>- |
| Information Security Audit | I | - Organization does not conduct any inter- nal or external information security audits. Network team has the responsibility to monitor the log records of the servers and take necessary action in case of any deviations. Organization does not have any information security certification |
| | II | - Case B has conducted an internal information security audit after defining the information security policy of the organization. Based on prescribed guidelines, this is for the first time that the CISO along with his team has conducted internal audits<br>- Organization also conducts external information secu- rity audits by Standardization Testing and Quality Certification (STQC) or any such CERT-In impanelled agency. These audits are generally network audits or application-specific audits. Based on the sensitivity of the applications and systems, different groups are mandated to maintain and monitor logs. |

| | | |
|---|---|---|
| Information Security Management Best Practices | I | - There is no clear plan for identifying and managing risks to various business operations of the organization.<br>- ISM practices of Case A are ad-hoc and reactive in nature.<br>- Assets are not clas- sified based on risk or criticality. PCs and laptops are generally used on shared basis, so it is hard to fix the accountability. |
| | II | - Organization follows layered security architecture, such as logged routers, Intrusion Prevention System (IPS), Intrusion Detection System (IDS) , layered firewalls, militarized zones, demilitarized zones, antimalware checks, proxy checks and antivirus system to protect its network<br>- follows a mechanism to categorize information infrastructure of the organization from 'highly critical' to 'not so critical |
| Information Security Incident Management | I | - No defined information security incident management plan.<br>- Organization follows a reactive approach towards information secu- rity incident management |
| | II | - Has an information security incident management plan defined and documented in the organiza- tion's information security policy document |
| Information Security Regulations Compliance | I | - Uses licensed software, downloading freeware software from the Internet is allowed and it is commonly practiced by employees. There is no mechanism to check the use of unauthorized software on company systems. Organization does not has any ISM certification (like ISO/IEC 27001 etc.)<br>- All the employees have access to all sorts of data. Even software developers take the project data and codes with them in their personal devices to home; there is no check or restriction on that. |
| | II | - Has full compliance to its policy related to the 'use of licensed software',<br>- Organization is planning to get an ISO/IEC 27001 ISM certification for its data centre.<br>- For the private, internal and sensitive data, organization uses various access control mechanisms, such as digital signatures and two factor authentication. |
| Information Security Management Effectiveness | I | - In absence of any information security policy or guidelines, there are no defined processes or systems for ISM in the organization<br>- In some cases, such incidents have delayed project delivery that resulted into adverse outcomes in terms of financial losses, loss of business and even losing clients. |
| | II | - The senior management finds the ISM practices of Case B effective, as they have not faced any serious security incident yet, except few minor defacement and Distributed Denial of Service (DDoS) attack cases.<br>- Organization has information security policy and guidelines in place; however, there is low level of compliance. |

## IV. CONCLUSIONS

This study adopts a qualitative research approach to review the ISM practices of IT—development and services companies. Findings of this study can be useful for organizations with similar nature of work or functions. Further, similar studies can be conducted for organizations from across different industries/ sectors. It would be interesting to see the influence of *organization size and industry type* on the varying nature of information security practices.

Correlations among various ISM factors can be identified to explore their causal relationships among each other. This may help to develop an organizational ISM framework which can be useful to prioritize various organizational ISM practices.

## REFERENCES

[1]. Alexandrova, M. (2015). Risk factors in IT

outsourcing partnerships: Vendors' perspective. Global Business Review, 16(5), 747–759.
[2]. Ashenden, D. (2008). Information security management: A human challenge? Information Security Technical Report, 13(4), 195–201.
[3]. Babbie, E. (2004). The practice of social research. Belmont, CA: Wadsworth/Thomson, Inc.
[4]. 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), 523–548.
[5]. Creswell, J. W. (1994). Research design—Qualitative and quantitative approaches. London, UK: SAGE.
[6]. Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transforma- tion case study. Computers & Security, 56(February), 63–69.
[7]. Doughty, K. (2003). Implementing enterprise security: A case study. Computers & Security, 22(2), 99–114.
[8]. Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. Computer Fraud & Security, 2005(11), 10–16.
[9]. Ernst & Young. (2010). Borderless security: Global information security survey. Retrieved 22 March 2015, from http://www.ey.com/Publication/vwLUAssets/Global_information_security_survey_2010_advisory/$FILE/GISS%20report_final.pdf
[10]. Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. Logistics Information Management, 15(5–6), 352–357.
[11]. ISO/IEC 27002:2005. (2005). Information Technology—Security techniques—Code of practice for information security management. Geneva, Switzerland: International Organization for Standardization.

Ashish Ukidve, et. al. "Analysis of evolution of information security management practices in organisations providing IT development & IT Enabled services." *International Journal of Engineering Research and Applications (IJERA)*, vol.11 (5), 2021, pp 18-24.