Article

Information Security Management Practices: Case Studies from India

Global Business Review
20(1) 253–271, 2019

DOI: 10.1177/0972150917721836
journals.sagepub.com/home/gbr

Abhishek Narain Singh[1]
M.P. Gupta[2]

Abstract

In recent years, information security has gained attention in organizations across diverse businesses and sectors. Primary reasons of this can be the new and innovative ways of information handling (during generation, processing, storage and distribution), and dependence of business processes on new and emerging IT/ICT mediums in organizations to carry out daily business activities. This has made organizations agile in terms of functioning and, at the same time, has posed new challenges. In this direction, the present study aims to explore and examine information security management (ISM) practices of two IT development and services organizations in India. In case study design, the study adopts qualitative research route to understand the current ISM practices of the case organizations. The observations derived from semi-structured interviews are presented using descriptive analysis methodology. Further, SAP-LAP (Situation, Actor, Process—Learning, Action, Performance) method of inquiry is used to analyse the findings from case studies. Results highlight the importance of consistent top management support, organizational information security culture and a proper monitoring system for ISM effectiveness in organizations. Insights derived from the study can be helpful for managers and decision makers in managing organizational information security practices.

Keywords

Data security, information security, information security management, case study, SAP-LAP

Introduction

With the increasing dependence of businesses over information and information system, it has become pivotal for organizations to protect their critical information assets against theft, loss or misuse. In recent times, the technical advancements, on one hand, have enabled organizations to process their business information in a faster, more effective and efficient way, it has also posed serious security threats and challenges for them. According to Ernst & Young's (2010) global information security survey,

[1] Assistant Professor, Institute of Management Technology Nagpur, Nagpur, Maharashtra, India.
[2] Professor and Head (Information Systems and E-Gov.), Department of Management Studies, Indian Institute of Technology Delhi, New Delhi, India.

Corresponding author:
Abhishek Narain Singh, Assistant Professor, Institute of Management Technology Nagpur, Nagpur, Maharashtra, India.
E-mail: singhabhi444@gmail.com

in 46 per cent cases companies have indicated that their annual investment in 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 equipped with the advanced technical solutions. However, technology alone is not sufficient to handle this problem. 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 any technical methods and managerial processes on the information resources (hardware, 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, tactical and operational) becomes essential (Ma, Schmidth & Pearson, 2009). Towards this direction, this article aims to understand and examine the ISM practices of two IT—development and services companies of India. The study uses the management lens while investigating the ISM practices of the cases under examination.

The next section of the article highlights the key studies and researches in the area. Third section discusses the methodology adopted for the study, followed by the key observations derived from the cases are discussed in fourth section. Fifth section presents the Situation, Actor, Process—Learning, Action, Performance (SAP-LAP) analysis of the cases. The next section discusses implications of the research findings for practitioners, followed by limitations of the present study and avenues for future research.

Literature Review

Information security is a multidimensional discipline (Posthumus & von Solms, 2004; von Solms, 2001). With the evolution of IT/ICT field and the advancements in the ways of information generation, processing, distribution/communication and storage, the nature of information security has changed accordingly. Information security has emerged as a separate discipline with multiple dimensions, such as physical security, technical security, operational security, mobile security, application security and behavioural security. von Solms (2001) identifies 12 different dimensions of information security and also explains the interrelationships among them.

The evolution of ISM discipline, as discussed by von Solms (2000, 2006), has happened into four waves. The first wave is the *technical wave*, where various tools and techniques were applied to handle various information security issues in the organization (the mainframe era where the build-in security features, such as user-id, passwords, and access control lists were prevalent). With the advancements of distributed computing World Wide Web and Internet, organizational boundaries have started blurring. This has led the evolution of the *management wave*, where information security got the attention of the board and senior management (von Solms, 2000). 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 wave, the *institutional wave* emerged. In the third wave, 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 wave* emphasized upon the corporate governance responsibility for the organizational ISM. The building blocks of the governance wave 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 maturity of ISM discipline, many frameworks for organizational ISM have been proposed (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 and von Solms (2006) discussed various strategic, tactical and operational factors building an information security governance model for organizations. According to the varying business requirements, organizations need a balanced mix of these factors to implement a robust ISM system (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 presents some of the organizational ISM case studies in varied contexts.

Table 1. Organizational ISM Case Studies

Author/s	Context	Methodology	Key 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
Zakaria (2004)	Information security culture challenges in a public sector organization in Malaysia	Questionnaire survey, semi-structured interviews and reviews of information security documents	Research design on security culture—identifying employees' information security behaviour
Mouratidis, Jahankhani and Nkhoma (2008)	Financial sector case study—large size bank	Questionnaire survey and interviews	Security concerns of general management have different perspective from network security personnel
Harnesk and Lindstrom (2011)	Analysing security behaviours in a public nursing centre	Interviews	Discipline and agility play vital role in shaping security behaviour

(continued)

Table 1. (continued)

Author/s	Context	Methodology	Key Findings
Singh, Picot, Kranz, Gupta and Ojha (2013)	ISM practices of Indian and German organizations	Semi-structured interviews	Industry type, organization size and culture and regulatory compliance are key determinants of ISM
Parsons, McCormac, Pattinson, Butavicius and Jerram (2014)	Information security vulnerabilities in three Australian government organizations	Web-based questionnaire survey and interviews	Key information security awareness concerns include wireless security, social media and reporting of security incidents
Dhillon, Syed and Pedron (2016)	Distractions in security culture after merger—two European telecom companies	Semi-structured interviews	Effective communication structure and defining clear group boundaries are paramount for ISM

Source: Prepared by the authors.

Methodology

In an interpretive case study research approach, this study examines the ISM practices of two IT—development and services organizations in India. Following the qualitative research route, semi-structured interviews were conducted to investigate the ISM practices of the companies. Purposive sampling technique was used to select interview respondents across the hierarchy in organizations to capture multiple viewpoints. Interviews were conducted personally, face-to-face in the real-life setting of the respondents. A semi-structured questionnaire template (given in Annexure) was used for the interview purpose. The template consists of 12 ISM factors identified from a previous study conducted by authors (Singh et al., 2014). These factors include *Information Security Requirements, Top Management Support, Information Security Policy, Information Security Training, Information Security Awareness, Information Security Culture, Information Security Audit, ISM Best Practices, Asset Management, Information Security Incident Management, Information Security Regulations Compliance* and *ISM Effectiveness.* Total 16 interviews were conducted, eight from each case organizations. Profiles of the respondents are given in Table 2. Each interview, approximately 45–50 minutes long, was audio recorded and transcripts were prepared for further analysis.

The study adopts a two-step methodology for data analysis and presentation. At first step, 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.

At second step, 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

Table 2. Respondents' Profile

	Profile of the Respondent	Work Experience
Case A	Managing Director (MD)	20 Years
	Manager—Software testing	10+ Years
	Project coordinator	6 Years
	Team lead—.(dot) Net	6+ Years
	Technical associate	5 Years
	Network engineer	2+ Years
	Network engineer	3+ Years
	Technical associate—Mobile applications	3 Years
Case B	General Manager—Infrastructure and Chief Information Security Officer (CISO)	23 Years
	General Manager—IT networks	25+ Years
	General Manager—Corporate coordination	27 Years
	Senior engineer—IT networks	15 Years
	Manager—Material management	12 Years
	Senior software engineer—E-procurement	7 Years
	Senior software engineer—Infrastructure and security	7 Years
	IT engineer	5 Years

Source: Prepared by the authors.

the key areas of improvements (Husain, Sushil & Pathak, 2002; Kak, 2004; Singh et al., 2013; Thakkar, Kanda & Deshmukh, 2008).

Case Study

Case A

Started in March, 2011, Case A is a New Delhi-based custom software solutions provider company. Company deals in developing and customizing software solutions for clients on a project basis and provides technical and business support in an outsourced capability. The main business and service areas of the company include IT consulting, web design and development, mobile applications development, software development, robotics and Internet marketing. The company has an employee base of 50 people, and it caters clients from a wide range of industries including aerospace, automotive, consumer goods, food, metal fabrication, medical, pharmaceutical and solar panel, among others.

Case B

Case B is an autonomous organization founded in July, 1986 that designs, develops, implements and maintains IT systems, products and services of one of the major government institutions in India. Governed by board, the organization has a Managing Director as the top authority. Operating with 800 employees, the key functions of the company are as follows provide IT solutions, manage overall information system and give IT consulting services to its parent organization. Headquartered in New Delhi, the organization has its regional offices in five other cities in India.

Key Observations

Key observations are presented based on the interview responses from employees across hierarchy in the case organizations. Questionnaire used for conducting interviews is given in Annexure.

Information Security Requirements

Since Case A operates in software development, web applications and mobile applications development business, any information loss (e.g., losing codes, software programs, applications, etc.) is crucial for the company and its operations. Any information security breach incident affects the productivity of the organization. This may ultimately 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. The top management and software developers acknowledge that information security is the critical aspect for business continuity of the organization.

> if the productivity is lost in our area, then it directly relates to losing our clients, because we have to deliver our projects within scheduled time. And if client loses the trust, he will not give us more business...

> ISM is beneficial for the organization as well as for the employees...

The core function of the Case B is the data and information management and to provide IT support to its parent organization for critical public functions. The survival of the organization is solely dependent upon the proper functioning of its information systems. Thus, information security is essential for Case B. Since customers of the Case B are citizens and the parent government organization, any deviation in data/information and information system will result in large public outcry. As described by the chief information security officer (CISO), 'if an internal application fails, only few users of departments will be affected, but if any of our critical application fails, it will be disastrous'.

> for my organization, there are two assets which are most important; one is the information which we hold and process, the second one, I will say, the technical human resources who do this job...

> my organization survives on managing information...

Top Management Support

Although the top management (of Case A) is aware of the importance of information security for the organization, a consistent support for the same is missing. This is primarily because of the budget constraints and reluctant approach of the senior management towards this issue. There is no information security officer or any similar authority in the company. ISM activities of the organization are managed by the network team. This leads to lack of co-ordination and control.

> time to time, there is top management support, but not up to the level what is required in our organization, it is lacking...

With the change in senior executives, there is a varying change in priority regarding information security in Case B. For some, information security is an important aspect, but for others, it is not. However, with

the newly created CISO position in the organization, information security has got attention and the ISM activities have started becoming streamlined. CISO along with his two team members are responsible to manage various ISM functions of the organization. Now with a push from CISO office, the senior management started realizing the importance of information security and is willing to support its various functions. Still, there is a challenge of lack of skilled manpower and funds to support various ISM functions in the organization.

> the situation was very bad. Now, it is in an improving stage. But it is not reached to a level where I feel satisfied. Still we have to beg for funds. So, it is still given a tertiary or later stage of priority... as the top manager feels about security the whole group feels like that only. So it is top to down always...

Information Security Policy

There is no documented information security policy in Case A. The information security roles and responsibilities of employees are not defined. There is no classification of accountabilities for various information security-related functions in the organization. In an ad-hoc manner, employees take actions on their own to manage information security related to their work.

Case B has released its information security policy in June 2012. Before that, there were some guidelines related to information security, but it was limited in sense and not covering all the aspects of ISM. Now, after June 2012, the organization has officially released a comprehensive information security policy which covers roles and responsibilities of employees, vendors and third-party contractors. There is a clause in policy to review it annually. According to CISO, 'we have identified certain areas of improvement in our policy and we are planning to incorporate them in our annual policy review'.

> comprehensive information security policy is there, but its compliance is another issue...

Information Security Training

There is no formal information security training programmes for employees (Case A)—neither at the time of joining the company nor later. There is no procedure for identifying information security requirements of employees as per their specific job requirements and accordingly train them. For any information security-related concern, employees take their own decisions. There is no formal procedure (predefined steps) or consulting authority. A need for regular information security training and awareness programmes were realized in the course of interviews with employees.

> there is no information security training or awareness program; it is based on individual efforts of employees...

> when employees join the company, all the criteria of ISM must be made clear to them, that what is information security? How we are managing it? And, how it is critical for us? Some briefing should be there for all the employees...

Case B has a defined process for information security training of employees. There are various internal as well as external information security training programmes for employees. Every group has a representative that coordinates information security activities of the group. There are two kinds of training—one is 'general awareness training' for every employee, and second is 'specific area related training' as

per specific job requirements. There is an internal team to coordinate the training programmes. Experts from industry and other agencies are invited to conduct training sessions, workshops and seminars. In addition to this, there is a 1 hour workshop conducted internally, where employees from different groups share their experiences related to ISM. For the area-specific training, employees are nominated from different groups and they have been trained by expert agencies, such as CERT-In (Computer Emergency Response Team—India) and ISACA (Information Systems Audit and Control Association), etc. CERT-In conducts such training programmes in every 15 days where generally 2–3 people participate from the Case B. These participants come back and share their learning within their group and with other groups through internal workshops in the organization.

> monthly we try to hold one hour workshop or lecture, where our group people or the people who have got the training in CERT-In, they share their experience. Or if some incident has happened in their group that we ask them to share...

> for most of them it is revelation (during training) that such things also keep happening...

Information Security Awareness

In the absence of any information security training programmes, employees in Case A found to be very less aware about various information security threats and countermeasures. Although some employees know the possible risks to the information and information assets that they are dealing with, but in the absence of any policy or guidelines, they have no idea what to do about it. There is no communication on information security roles and responsibilities of employees. There is a general lack of awareness about penalties or legal consequences of any information security breach incident. There is no advisor to consult/discuss ISM concerns and issues in the organization.

> without employees' awareness for information security, budget and all other resources and efforts are useless...

> time to time sessions on information security will be beneficial for all employees...

Case B makes efforts to communicate possible risks, threats and countermeasures to employees through various training programmes conducted internally as well as outside the organization. Along with this, organization has a comprehensive information security policy that is been discussed with employees on time to time. Organization's information security policy and guidelines are published on the Intranet and employees are asked to refer to it in case of any confusion. There is an internal mailing system where employees raise and discuss ISM-related issues/concerns. Further, as next step, every employee has to sign a compliance declaration for organization's information security policy. Employees are being educated on their acceptable behaviour towards organization's equipment, network, etc. In this direction, CERT-In acts as a government appointed advisor for various ISM activities and functions of the organization.

> I will not say, 100 per cent are aware. It might be 50-50. But we are trying to improve that situation by bringing more people in the training groups...

> right now, more focus is on creating awareness, that, it is important. Then, we will focus on specifics...

Information Security Culture

Case 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. For example, 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 is no mechanism to monitor employees' information security behaviour. Organization does not have any forum to discuss these issues. If anyone faces some problem, they take ad-hoc actions within group to resolve the issue.

> I give suggestions sometimes, but this is not my job...

> they (employees) think, it (ISM) is a simple thing, who cares? Nobody bothers about it. The approach is, who will need it, will do it; my job is to do my work...

With the help of regularly conducted information security training and awareness programmes, Case B has an information security culture, but in a very nascent stage. Still it needs a wide spread within the organization, not only among employees but also in the attitude of senior management and executives. The groups which are dealing with critical or sensitive applications are generally found more aware than others. The CISO estimates the information security awareness level in organization as 50 per cent. Thus, it can be said that there is still a long road to travel. There are further plans to start a forum where employees can exchange their ideas and share their concerns with senior officials regarding ISM.

> some people are very good in following security policies. We find around 20 per cent of such people. Another 30 per cent will be on the fringes, if they are told, they will follow. Rest 50 per cent, they don't care. They feel their things are not so critical. …Basically, it comes from the culture. The high security culture is not yet there, I'll say, it's still in a low state...

Information Security Audit

There is no mechanism of information security audit in Case A. Organization does not conduct any internal 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. As described by the Managing Director of the company, 'we are a small company; we do not require any such ISM certification. May be in future, as the company grows, we will consider it'.

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. These guidelines are in the form of a checklist (generic as well as application-specific) derived from multiple agencies, such as CERT-In and ISACA. As per the policy, internal audit is to be conducted once every year. It is the responsibility of representatives from various groups to coordinate audits with the security team. Organization also conducts external information security 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.

> May be by next year, we are planning to have ISO/IEC 27001 security certification for our data centre at-least, not for the organization as a whole, because there are lot of processes which are not yet correct...

Information Security Management Best Practices

ISM practices of Case A are ad-hoc and reactive in nature. There is no clear plan for identifying and managing risks to various business operations of the organization. Some of the gap areas, as highlighted, include the following absence of any risk management plan, sharing of passwords, no filtering of Internet downloads, no regular updates of antivirus programmes, employees take with them sensitive project data files. This may partially be because of poor information security and no thrust from top management.

> they feel bounded if there is proper implementation of security systems. For example could not use pen drives, could not take codes home with them, could not put data of their own, not be able to open private emails, etc.

Case B does not have any risk management plan for the organization. Based on the criticality of applications, different groups are required to identify risks and define their mitigation plan. It depends upon the initiatives taken by group head; there is no defined process for this, as of now. 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 against malicious programmes and cyber-attacks. Best-practices guidelines, as part of security policy, include the following asset classification, clean desk policy and changing passwords periodically among others.

> in security policy all these things are very clearly and elaborately mentioned. They have to take care of the security of their assigned equipment, desks, etc.

Asset Management

As a part of inventory, Case A keeps record of the company's IT and non-IT assets. Assets are not classified based on risk or criticality. PCs and laptops are generally used on shared basis, so it is hard to fix the accountability. There is no process to identify the critical risks for the information and information assets of the organization. Organization does not have any physical access control mechanism; employees have free access to different functional areas. There is no electronic or manual identity check (and record keeping) while entering or exiting the office. Although bringing personal data computing or storage devices to the office is not allowed, there is no check for the same. It was found in the course of interview that there is no strict implementation of such rules. While network team has been assigned the task to restrict the access of IT systems and services based on roles, all the systems including central server are generally accessible by all the employees. Everyone has passwords and can log-in to the server and other systems.

> BYOD is not allowed, but there is no check. If they want, they can bring… everyone brings his/her pen drives and uses it on systems…

Case B follows a mechanism to categorize information infrastructure of the organization from 'highly critical' to 'not so critical'. The categorization is carried out based on the basis of risks, threats and the cost of recovery. Organization also follows various physical security access control mechanisms, such as video surveillance at entry gates and data centres, RFID-controlled doors, entry only with proper ID card and restricted access to various areas/departments within the office. For employees to access the IT systems and services of the organization, there are various roles defined based on the privilege levels assigned to them.

> in future, we plan to have a single ID authentication, so that the roles or privileges being decided from a single place. Right now, it is completely distributed..

Information Security Incident Management

During interviews, it was found that Case A has no defined information security incident management plan. Employees are not aware of the consequences of not following information security processes or practices. As a business continuity and disaster recovery plan, organization uses a centralized server for data storage, but the access password is shared among employees. The company uses free online storage spaces (e.g., Dropbox) for backup. Organization follows a reactive approach towards information security incident management. Following is one such incident as described by an interviewee:

> few days ago an employee formatted a partition of the system hard disk by mistake. There are mechanisms like recovery software to prevent such things, but they are not taking care about this. We lost a lot of our data and test applications. I lost my R&D data for some test application… such incidents delay the projects… many developers are complaining to me that they lost their data. Such incidents de-motivate the R&D work...

Case B has an information security incident management plan defined and documented in the organization's information security policy document. The implementation and compliance of which is dependent upon various application groups. Few groups which deal with critical and sensitive applications have created and communicated the incident management plan, whereas few others are reluctant towards it. As described by a group head, 'it requires a compliance pressure from the top, which is not yet there'. Since the whole ISM process has started recently in the organization, the management's focus is to first create more awareness and slowly proceed to more specific objectives. Organization has a Business Continuity (BC) and Disaster Recovery (DR) site at a distant geographical location. There is a defined process to take regular data backups which is stored separately off-site.

Information Security Regulations Compliance

Although Case A 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.) and nor does it planning to have it in near future. Regarding the data privacy issues, on principle, different groups are allowed only to access the data and other relevant information related to their specific work/project, but in practice, 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.

> for any certification, you need policies and proper documentation of every process, that's not there...

> actually in our system, there is no privacy. As I said, anybody can take the codes to his/her home, if he/she wants...

For the servers' front, Case B has full compliance to its policy related to the 'use of licensed software', whereas for the standalone PCs, there is no strict compliance to the 'use of licensed software' policy.

There is no mechanism to check the validity of the licenses of software used on PCs; however, the organization is planning to have an automated tool for the same in the next upgrade of its network access control. Organization is planning to get an ISO/IEC 27001 ISM certification for its data centre. For information security certification at organizational level, CISO has a view that they are not yet ready for the same. As most of the data of Case B is public in nature, organization does not have much privacy concerns. Whereas, for the private, internal and sensitive data, organization uses various access control mechanisms, such as digital signatures and two factor authentication.

> we want to go step by step. Let me see how much of effort and infrastructure investment is there, and then we will plan accordingly for ISM certification...

Information Security Management Effectiveness

Although the top management, managers and other employees of Case A acknowledge the fact that information security is a critical aspect of their business, the issue has given very low priority in the organization. In absence of any information security policy or guidelines, there are no defined processes or systems for ISM in the organization. Due to lack of training or awareness programmes, employees are generally unaware about various risks to the information and information assets that they are dealing with. In the course of interview, this has come-up very clearly that because of the carelessness and reluctance, often data get lost, and this affects the overall productivity of the organization. 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.

> a risk assessment and management plan is definitely required for the organization, but it is not there...

> accountabilities need to be set, and not just verbally, it should be defined and documented...

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. Organization has information security policy and guidelines in place; however, there is low level of compliance. To reduce human intervention, there is a need of automated systems to enforce compliance. More awareness is needed at higher management and at board level to bring information security up in the priority list, so that required resources in terms of funds and man-power are made available.

> in our current case, security is actually a hindrance to the performance… that is the feeling of top management in-general...

> we feel that our security systems and practices are working. But they are not in compliance to our policy fully...

SAP-LAP Analysis of Cases

Case A

The 'Situation, Actor, Process—Learning, Action, Performance' (SAP-LAP) analysis of Case A (Table 3) shows that the ISM practices of the company are ad hoc in nature. In absence of any information security policy and lack of training/awareness programmes for employees, there is no information

Table 3. SAP-LAP Analysis of Case A

SITUATION	No documented information security policy
	No information security training for employees
	No internal or external information security audits
	Poor awareness for information security; individual level efforts
	No privacy for clients' data, everyone can access every project information
	No password policy, administrative passwords are shared with employees
	No clear division of work, responsibility and accountability
ACTOR	Managing Director
	Network team
	Group (team) leaders
	Employees
	Clients
PROCESS	No risk management process
	No asset management
	Reactive approach towards ISM
	Ad-hoc approach for information security incident management
	No documentation, records or logs are maintained
LEARNING	If the top management shows concern about information security, rest follow and vice versa
	Fixing responsibilities and accountabilities can create an environment for good ISM practices
	Even basic awareness can help to reduce big information security incidents
	A blame-game creates bad information security culture in organization
	No action for information security violations encourage employees to do the same in future
ACTION	Make an information security policy (and guidelines) and roadmap for its implementation and compliance
	Identify information security risks for the organization and their counter measures
	Provide general information security training to employees at the time of joining and further application-specific training to different teams
	Educate employees for their acceptable/unacceptable behaviour regarding information security
	Non-disclosure agreements for employees and third parties
PERFORMANCE	Information security incidents affect the productivity of organization
	Loss of data/information hinders R&D activities and de-motivate employees
	Data losses and information security breach incidents lead to lack of trust and dissatisfaction in clients
	Because of bad ISM practices (resulting into project delays), organization may suffer loss of business
	Breach of data/privacy can create legal complications for the organization

Source: Prepared by the authors.

security culture in the organization. Learning derived from the case suggests that organization needs to identify key risks and vulnerabilities to its information and information assets, and accordingly define an information security policy and implementation mechanism. This will certainly help organization to improve in terms of productivity, employees' satisfaction and clients' trust.

Case B

The findings from SAP-LAP analysis of Case B (Table 4) suggest that the organization started streamlining its ISM practices; however, it is still in a nascent stage. A consistent top management support is

Table 4. SAP-LAP Analysis of Case B

SITUATION	Information security has given a tertiary level priority
	Top management shows the support, but it is not consistent
	Recently released information security policy
	Lack of resources (budget and skilled manpower)
	Reactive approach most of the time
	Information security awareness among employees: 50-50
	Management feels that 'security is actually a hindrance to the performance'
ACTOR	Top management (Board)
	Chief information security officer and two team members
	Group-wise information security representatives
	Network team (to manage IT infrastructure)
	CERT-In, STQC, ISACA (for conducting training programmes and audit)
	Vendors and contract employees
	Clients/customers
	Employees
PROCESS	First internal information security audit conducted recently
	Periodic general information security awareness training and specific area-related training
	Monthly internal workshop for sharing groups' information security experience
	No risk management process, based on efforts of individuals and group head
	Network logs are generated and monitored on daily basis
	Asset classification based on risk, chances of occurrence and cost of recovery
LEARNING	Internal threats (ignorance, carelessness and malicious intent) are as challenging as external threats
	Internal information security audit has revealed vulnerabilities in the system
	Building an information security culture is must for good ISM practices in organization
	As the top manager feels about information security, the whole group follows the same
ACTION	Specialized training according to the specific job requirement
	Declaration from all the employees that they have read and understood the information security policy and guidelines
	Creation of an information security forum for management and employees
	Building information security into operational systems
	ISO/IEC 27001 ISM certification for data centre
	Implementation of a single ID authentication system
	A disaster recovery site to ensure business continuity
PERFORMANCE	Top management needs to give more priority to information security issues of the organization
	Availability of required resources in terms of budget and manpower to streamline various ISM functions in the organization
	A defined risk assessment and management plan to ensure the protection of organizational information assets against internal and external threats
	Compliance enforcement for organizational information security policies and guidelines to build an information security informed workforce

Source: Prepared by the authors.

essential to gradually take it to a mature level. Moreover, a regular monitoring is essential to improve the level of information security compliance among employees in the organization.

Discussion

Fast pacing technological advancements provide new and innovative ways to businesses to conduct their daily operations, such as collaboration, coordination, product/service—design, development and delivery, and providing alternate ways to connect and communicate with different stakeholders. In this pursuit, modern day organizations have become over dependent on IT/ICT for their various business functions. In case of some businesses, it has become nearly impossible to conduct daily operations without proper functioning of their information systems. In such a scenario, protecting business information and related assets from external as well as internal threats have become a matter of paramount importance for organizations. To deal with this situation, on one hand, organizations are relying more and more on the usage of advance technological solutions, the management issues are often overlooked (Pricewaterhouse Coopers, 2012).

As evident from the cases, it is the responsibility of board and top management to design and develop information security strategy in accordance to the business objectives of company. Aligning information security goals to the business objectives of the organization is the key to success of organizational information security strategy (Kayworth & Whitten, 2010). Having a comprehensive information security policy is the first step towards this direction. As reflected from Case A, in absence of any information security policy (and guidelines), there are no clearly defined roles, responsibilities and accountabilities towards organizational information and information asset, making them prone to information security risks and threats. It is the responsibility of management to make employees aware of the policies, guidelines, risks and countermeasures through regular training and awareness programmes (Abouzeedan & Busler, 2006). Once the policy is in place, employees need to be educated on their acceptable behaviour towards organizational information systems. Monitoring compliance to organizational information security policies and guidelines through periodic internal as well as external audits gives confidence to the management and also indicates the areas of improvement. Without compliance monitoring, it is hard to assess the current status of the maturity of organizational ISM practices (Kankanhalli et al., 2003), as also evident in case of Case B. It is essential to provide a platform to share the good practices within various teams or groups inside the organization. This helps in peer learning and sharing of best practices across organization and helps in building a security culture (Zakaria, 2004).

In a fast-changing threat scenario, organizations need to be dynamic and up-to-date with the current industry standards and ISM best practices. Again this is the responsibility of board and top executives to draw an organization-wide information security and risk management plan that spans across strategic, tactical and operational levels. Top management support (for budget and man power) is crucial along with regular monitoring and review of organizational ISM practices (Eloff & Eloff, 2005). Organizations need a clearly defined disaster recovery and business continuity plan, discussed with all relevant stakeholders, for incident management. In addition to this, employees need to be made aware and educated about the action plan in case of any information security breach incident. Mostly, organizations are reactive to such cases rather than being proactive, evident from Cases A and B. Such incidents can result into loss of business information and productivity impacting organization's relationship with clients and its repute. Post-incident analysis—identifying vulnerabilities, fixing accountabilities and making suitable changes in policies and processes—plays a vital role for future preparedness (Ahmad, Maynard & Shanks, 2015).

Conclusion

The present study adopts a qualitative research approach to understand and examine the ISM practices of two IT—development and services companies in India. Semi-structured interviews and descriptive analysis methodology followed by SAP-LAP method of inquiry have been used to analyse the cases under study. Findings of the study are limited to the two case organizations under study and cannot be generalized. However, this can be useful for organizations like in domain 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 effect of *industry type* and *organization size* on the varying nature of information security practices. As an extension of this study, linkages among various ISM factors can be identified to explore their causal relationships among each other. Further, this may help to develop an organizational ISM framework which can be useful for practitioners to prioritize various organizational ISM practices.

Annexure

ISM Questionnaire Template

1 Information Security Requirements

1.1 Do you think that information is a critical important business asset for your organization?

1.2 For what purposes Information Security (IS) is important? For what reasons; e.g. operations, intellectual property, etc.?

1.3 At what level, an IS breach incident can affect the business activities of the organization (e.g. impact on certain operations or overall business, etc.)?

2 Top Management Support

2.1 Is the top management concerned and shows support for IS requirements and activities of the organization? If yes, how?

2.2 Are the required resources (budget, manpower, technology) made available to fulfil organization's security requirements?

3 Information Security Policy

3.1 Does the organization has an IS policy? If yes, specific or as part of IT policy?

3.2 Does the IS policy specify roles and responsibility of employees (e.g. accountability)?

3.3 Is the organization's IS policy been regularly reviewed for effectiveness and completeness? If yes, by whom, what is the procedure for it?

3.4 Does the organization has an IS policy for contractors/third party vendors?

4 Information Security Training

4.1 Does the organization conduct IS training for employees? If yes, by whom, and how frequently?

4.2 Are the training programmes useful, up-to-date and cover specific job requirements of employees?

4.3 Does the organization has a dedicated IS steering committee responsible for IS training of employees? If yes, who are the members and what are their roles?

5 Information Security Awareness

5.1 Are IS objectives, policies, risks, roles and responsibilities communicated and discussed with employees? If yes, what are the ways of communication?

5.2 Are employees been educated on their acceptable behaviour? Are penalties and legal consequences of non-compliance discussed with employees?

5.3 Is there an IS advisor to coordinate various ISM activities?

6 Information Security Culture

6.1 Do employees see and practice IS as a part of their job or it is an additional burden that hinders their work?

6.2 Does the organization has some formal procedures to build IS into operational systems?

6.3 Does the organization have any forum to discuss and resolve employees' IS concerns/issues and give management direction and support?

7 Information Security Audit

7.1 Is there a process for monitoring and making logs of access record of the critical systems/applications?

7.2 Does the organization has a process to review the compliance of its information system with organizational IS policies and guidelines?

7.3 Does the organization conduct internal IS audits? If yes, what are the roles, processes, structure of audit team, and frequency of such audits?

7.4 Does the organization conduct external IS audits by an independent third party? If yes, how frequently?

8 Information Security Management Best Practices

8.1 Does the organization has an IS risk management plan (to identify, assess and review risks, and archive the action taken)?

8.2 How does the organization protect its software, hardware, and information against virus, malware and cyber-attacks?

8.3 Tell about IS good practices of your organization (e.g. security measures for e-commerce, shred sensitive documents which is no longer needed, back-ups of critical information and databases, password policy, etc.)?

9 Asset Management

9.1 Does the organization have an information asset classification system (based on ownership, level of confidentiality, etc.)?

9.2 Does the organization make an effort to determine the critical risks of its information assets?

9.3 Does the organization have a physical access security control mechanism (e.g. security check at entrance, controlling access to secured/restricted areas)?

9.4 Does the organization has an access control mechanism for IT systems and services (e.g. authentication check, access rights, privilege levels, account creation/deletion rules, and authentication for external connections)?

10 Information Security Incident Management

10.1 What risk mitigation techniques organization follows to secure its information assets?

10.2 What steps to take to respond to an IS incident (e.g. reporting, actions, roles, documentation, review, suitable changes in policies and guidelines, etc.)?

10.3 Does the organization have a business continuity and disaster recovery plan to ensure speedy resumption of its essential operations?

11 Information Security Regulations Compliance

11.1 Does the organization have a mechanism to comply with software licenses? How does it prohibit the use of unauthorized software?

11.2 Does the organization comply with any international ISM standards e.g. ISO/IEC 27001, COBIT, etc. or have any such IS certification?

11.3 How the organization protects privacy of data/information of its employees/clients? Are the non-disclosure-agreements discussed and signed with employees/contract persons?

12 Information Security Management Effectiveness

12.1 Do you think organization's IS policies and guidelines are effective? If no, suggest drawbacks and areas of improvement?

12.2 Do you think organization follow adequate processes to operationally enforce IS policies/guidelines? If no, suggest drawbacks and areas of improvement?

12.3 Is there a process to review organization's IS policies, guidelines and procedures? What events cause a change/update in current IS practices of the organization?

Acknowledgement

The authors are grateful to the anonymous referees of the journal for their extremely useful suggestions to improve the quality of the article. Usual disclaimers apply.

References

Abouzeedan, A., & Busler, M. (2006). Information technology (IT) and small and medium-sized enterprises (SMEs) management: The concept of 'firm impact sphere'. *Global Business Review*, *7*(2), 243–257.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717–723.

Alexandrova, M. (2015). Risk factors in IT outsourcing partnerships: Vendors' perspective. *Global Business Review*, *16*(5), 747–759.

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201.

Babbie, E. (2004). *The practice of social research*. Belmont, CA: Wadsworth/Thomson, Inc.

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.

Creswell, J. W. (1994). *Research design—Qualitative and quantitative approaches.* London, UK: SAGE.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, *56*(February), 63–69.

Doughty, K. (2003). Implementing enterprise security: A case study. *Computers & Security*, *22*(2), 99–114.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10–16.

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

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.

Harnesk, D., & Lindstrom, J. (2011). Shaping security behaviour through discipline & agility: Implications for information security management. *Information Management & Computer Security*, *19*(4), 262–276.

Hong, K., Chi, Y., Chao, L., & Tang, J. (2006). An empirical study of information security policy on information security elevation on Taiwan. *Information Management & Computer Security*, *14*(2), 104–115.

Husain, Z., Sushil, & Pathak, R.D. (2002). A technology management perspective on collaborations in Indian automobiles industry: A case study. *Journal of Engineering Technology Management*, *19*(2), 167–201.

ISO/IEC 27002:2005. (2005). *Information Technology—Security techniques—Code of practice for information security management*. Geneva, Switzerland: International Organization for Standardization.

Kak, A. (2004). Strategic management, core competence and flexibility: Learning issues for select pharmaceutical organizations. *Global Journal of Flexible Systems Management*, *5*(4), 1–16.

Kankanhalli, A., Teo, H. K., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, *9*(3), 163–175.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors. *International Journal of Information Management*, *24*(1), 29–42.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Morrow, D. W. (2006). The top information security issues facing organizations: What can government do to help? *Information Security and Risk Management*, *34*(4), 1–10.

Ma, Q., Schmidth, M. B., & Pearson, J. M. (2009). An integrated framework of information security management. *Review of Business*, *30*(1), 58–69.

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580–584.

Mouratidis, H., Jahankhani, H., & Nkhoma, M. Z. (2008). Management versus security specialists: An empirical study on security related perceptions. *Information Management & Computer Security*, *16*(2), 187–205.

Musa, A. A. (2010). Information security governance in Saudi organizations: An empirical study. *Information Management & Computer Security*, *18*(4), 226–276.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organizations. *Information Management & Computer Security*, *22*(4), 334–345.

Perks, C., & Beveridge, T. (2003). *Guide to enterprise IT architecture*. New York, NY: Springer-Verlag.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646.

PricewaterhouseCoopers. (2012). *Global state of information security survey*. Retrieved 17 November 2014, from http://www. pwc.com/jg/en/media-article/2012-global-state-of-information-security-survey.jhtml

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, *27*(5), 644–667.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225–239.

Sushil. (2000). SAP-LAP models of inquiry. *Management Decision*, *38*(5), 347–353.

———. (2001). SAP-LAP models. *Global Journal of Flexible Systems Management*, *2*(2), 55–61.

Thakkar, J., Kanda, A., & Deshmukh, S. G. (2008). Interpretive structural modeling (ISM) of IT-enablers for Indian manufacturing SMEs. *Information Management & Computer Security*, *16*(2), 113–136.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11.

von Solms, B. (2000). Information security—The third wave? *Computers & Security*, *19*(7), 615–620.

———. (2001). Information security—A multidimensional discipline. *Computers & Security, 20*(6), 504–508.

———. (2006). Information security—The fourth wave. *Computers & Security*, *25*(3), 165–168.

von Solms, R., & von Solms, B. (2006). Information security governance: A model based on the direct-control cycle. *Computers & Security*, *25*(6), 408–412.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4–19.

Zakaria, O. (2004, November 26). *Understanding challenges of information security culture: A methodological issue*. In 2nd Australian Information Security Management Conference, Perth, Western Australia, pp. 83–93.