CHAPTER: LITERATURE REVIEW

2.1 INTRODUCTION
Before going for a detail design of this research, it is better to have a clear understanding of the areas such as information, information security, Information Security Policy, job stress and the literature related to the study. Therefore, this chapter is written down to fulfill that requirement.

2.2 WHAT IS INFORMATION
The concept of information in an organization context is more complex and difficult than the frequent use of this common word. Information in this context can be defined as the transformation of data, which will be interpreted and understand by the recipient of the message (Lucey 1997, p14).

Information has many characteristics, which can be classified in numerous ways such as
1. By Source e.g. internal, external, primary, secondary etc
2. By Nature e.g. quantitative, qualitative, formal, informal etc
3. By Level e.g. strategic, tactical, operational etc
4. By Time e.g. historical, present, future etc
5. By Frequency e.g. continuous (real time), hourly, daily, monthly, annually etc
6. By Use e.g. planning, control, decision making etc
7. By Form e.g. written, oral, visual, sensory etc
8. By Occurrence e.g. at planned intervals, occasional, on demand etc
9. By Type e.g. detailed, summarized, aggregated, abstract etc

Good information matters rather than bulk information, good information is that which is used and which creates value. Experience and research showed that good information has numerous qualities as such relevant, accurate, and complete enough for its purpose, confidence about the source, communicate to right person in right time with the right level of details, communicated by an appropriate channel of communication and understand by the end user (Lucey 1997, p18).
In summary information is knowledge and understanding that is usable by the recipient. It reduces uncertainty and has surprise values and it must tell the recipient something not already known which could not be predicted. (Lucey 1997, p14).

2.3 INFORMATION SECURITY

Information in organization context may differ from organization to organization and, importance and critical level of it may depend on the recipient and recipient’s requirement. Security of the organization’s secret information comes to the picture when consider about recipient, who has received such information and recipient’s requirement.

There are three widely accepted elements of information security namely Confidentiality, Integrity and Availability (Nevada, 2009).

2.3.1 Confidentiality

Confidentiality can be defined as preventing disclosure of information to unauthorized individuals or systems. The International Organization of Standardization (ISO) has regarded confidentiality, or secrecy, to be the key element of information security and ISO clearly states ensuring that information is accessible only to those authorized to have access is the basis of maintaining secrecy about any information. If secret information is disclosed to competitor’s hand that can be a biggest threat to any organization (Hopkings, 2006).

2.3.2 Integrity

In fact, data integrity is to maintain the accuracy of the data while it is in operation, storage and more importantly when it is being transferred. Most illegal steps and cyber crimes take place during the transfer process. Therefore, if the basic honesty in data integrity is violated, information security cannot be sustained. Integrity is violated when an employee accidentally or with malicious intent deletes important data files in a computer system, manipulating, or destroying important data in hard documents (Hopkings, 2006).
2.3.3 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. Therefore, the basic definition for availability of information should be available to the right person when information is needed (Hopkings, 2006).

As discussed above organizations can manage and protect their confidential information by ensuring data confidentiality, integrity, and availability according to the ISO17799 and BS799 standards (Tong, et al. 2003).

Information security is a critical issue threatening organizations worldwide. With modern national economies and businesses fully dependent upon information technology for survival, the need to protect information is more paramount than ever before.

Fitzgerald (1995) has identified ten key controls as the fundamental building blocks for the development of information security and should be implemented first. These ten key controls are as follows.

1. Information Security Policy document
A written policy document must be available to all employees responsible for information security.

2. Allocation of security responsibilities
Responsibilities for the protection of individual assets and for carrying out specific security processes must be explicitly defined.

3. Information security education and training
Users must be given adequate security education and technical training.

4. Reporting of security incidents
Security incidents must be reported through the correct channels as quickly as possible.

5. Virus control
Virus detection and prevention measures and appropriate user awareness must be implemented.
6. Business continuity-planning process
There must be a managed process in place for developing and maintaining business
continuity plans.

7. Control of proprietary copying
Copyright material must not be copied without the owner's consent.

8. Safeguarding of company records
Important records must be safeguarded from loss, destruction, and falsification.

9. Compliance with data protection legislation
All applications handling personal data must comply with data-protection legislation
and principles.

10. Compliance with security policy
Systems must be regularly reviewed to ensure compliance with security policies and
standards.

Today organizations have become increasingly depend on information systems for
strategic advantage. Therefore, the issues of information systems security have
become more important. It has become necessary on investing on information system
security to prevent from abuses, which may lead to competitive disadvantage (Gupta
and Hammond, 2005).

Ban and Heng (1995) examined the issues facing the provision of computer security
in the Small and Medium Enterprises in Singapore. As per their study, issues that
SMEs may face in their implementation of computer security may include
sophistication of computer usage, scale of computer operation, lack of resources and
technical specialists, computer used primarily for mundane and non-critical operations
and cost of standard PC hardware and common office software.

In the context of Sri Lankan telecommunication sector, there is a huge competition
going on among eight telecommunication Service providers for attracting new end
users for their services. Due to high competition in the industry, every organization
may anticipate finding out competitor is marketing strategies and before they put them
into the market. Therefore, telecommunication service providers have given a special
attention to information security concepts for protecting their own marketing
strategies and company secrets.
2.4 INFORMATION SECURITY POLICY

For decades, information has been considered as a valuable corporate asset for any organization, which enables to add value to its products and services, reduces costs, meet customer requirements, and attract new customers for their products and services.

Solid security products or technologies alone cannot protect critical information in any organization; there should be a properly implemented policy to manage such information (Chang and Ho, 2006).

Information Security Policy is a set of controls and procedures adopted by particular organization to provide adequate protection to maintain confidentiality of their information. This information can be in any form such as electronic, printed, and recorded voice (Danchev, 2003).

In a research study carried out in Taiwan, Information Security Policy is defined as a policy targeting specifically at improving an organization’s information security level. Further IS policy is described in that as follows (Hong, et al. 2006).

1. The rules set-up for the use of information assets, and the statement set-up for the security priorities to achieve organizational objectives.
2. The guideline for the scope of information security.
3. The principle for information management and resource use.
4. The principle for supporting security techniques.

Information Security Policies are documented and made available to all employees to have a clear understanding of it. Within an organization, these written policy documents provide a high-level description of the various controls and procedures, which will be used to protect the information. Further these policies and procedures may differ from organization to organization depends on their requirements.

Contents of an Information Security Policy Document

Contents may be differing from organization to organization and ideal Information Security Policy document may contain the following elements (Danchev, 2003).

1. Title - Brief description of the document.
At the Information Security Policy formulation level, writing an IS policy plays a major role, which should cover the administrative, technical, management and legal requirements.

For example, if an organization has identified the threat of information theft and the vulnerability is the weak implementation of the user password for critical system, affecting confidentiality of the information, then the action plans should outlined as

1. Administrative: Provide appropriate training.
2. Technical: Enforce strong password selection through appropriate parameters.
3. Management: Ensure that the password policy is approved by management. Ensure user acceptance by asking them to sign appropriate form.
4. Legal: Define disciplinary action (Kadam, 2007).

An empirical study of Information Security Policy on information security elevation in Taiwan proved that implementing information security polices is elevating organizational information security level. As per their findings it is recommend, if an organization is in the hope of elevating its organizational information security, building or adopting an IS Policy may be an effective managerial measure to achieve that target (Hong, et al 2006).

### 2.5 INTERNATIONAL STANDARDS FOR IS POLICY

Information Security Policy has attained an international awareness and several international standards have been built already. As shown in Table 2.1, these six standards could be useful reference while establishing an IS Policy (Hong, et al 2006).
<table>
<thead>
<tr>
<th>International standard</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS 7799 (Code of practice for ISM)</td>
<td>Describe the minimum contents in an IS Policy. Explain what should be done with an IS Policy. An IS Policy should be approved by management. Published and communicated throughout the organization. An IS Policy should be evaluated and updated periodically.</td>
</tr>
<tr>
<td>ISO/IEC 17799</td>
<td></td>
</tr>
<tr>
<td>BSI IT baseline protection manual</td>
<td>Description of drawing up an IS Policy Coverage topics. Contents Review.</td>
</tr>
<tr>
<td>COBIT (The information system audit and control association and foundation, ISACAF)</td>
<td>Describes the process and control needs for implementing an IS Policy. Brief section on the security and internal control framework policy. Writing and maintaining a document</td>
</tr>
<tr>
<td>GASSP (Generally accepted system security principles)</td>
<td>Minimal requirements for an IS Policy and principles behind it. The different processes needed for defining, maintaining and implementing the policy The hierarchy concept of an IS Policy.</td>
</tr>
<tr>
<td>GMITS (ISO/IEC PDTR 13335-1)</td>
<td>Provide a comprehensive guidance on information security with planning, management and implementation.</td>
</tr>
<tr>
<td>ISFs Standard of good practice (The globally representation information security forum, ISF)</td>
<td>Performance evaluation. List the contents of IS Policy. The characteristics of the IS Policy. Explain the acceptable user behavior.</td>
</tr>
</tbody>
</table>

The procedures for building an Information Security Policy could be summarized as mentioned in an empirical study of Information Security Policy on information security elevation in Taiwan (Hong, et al 2006).

1. Project initiation
2. Security policy development
3. Consultation and approval
4. Security awareness and policy education
5. Disseminate policies

2.6 JOB STRESS

Job Stress is defined as an adaptive response to an external situation that results in physical, psychological, and/or behavioral deviations for organizational participants (Luthans, 2008).
The stress response is a mobilization of the body’s natural energy resources when confronted with a stressor in his or her environment. A stressor may be defined as any “demand made by the internal or external environment that upsets a person’s balance and for which restoration is needed” (Larson, 2004).

Further stress can be considered as good stress or bad stress. Bad stress could result from an unpleasant situation such as losing one’s job. An example of good stress would be a situation that creates excitement, stimulation, and arousal for the individual. A job promotion might be an example of a positive, invigorating type of stressor. Any type of stress puts a strain on the person. However, good stress results in a less negative effect on the person (Selye, 1976).

Job stress may lead to dissatisfaction of the job, to poor work performance or even injury further this is also associated with various biological reactions that may lead ultimately to compromised health, such as disease, or in extreme cases death (NIOSH, 2009).

Cooper and Marshall (1976) original model of work-related stress included five sources of stress at work, such as

1. Intrinsic to the job, including factors such as poor physical working conditions, work overload or time pressures
2. Role in the organization, including role ambiguity and role conflict
3. Career development, including lack of job security and under/over promotion
4. Relationships at work, including poor relationships with your boss or colleagues, an extreme component of which is bullying in the workplace
5. Organizational structure and climate, including little involvement in decision-making and office politics (Johnson, et al 2006).

Stress is associated with impaired individual functioning in the workplace. Negative effects include reduced efficiency, decreased capacity to perform, dampened initiative and reduced interest in working, increased rigidity of thought, a lack of concern for the organization and colleagues, and a loss of responsibility (Fairbrother and Warn, 2003).
Further Stress has been associated with important occupational outcomes of job satisfaction, organizational commitment, and employee withdrawal behavior. Mainly work related increase may have a direct impact to performance of the employees.

There are many causes or stressors, which are affecting to the job stress of the employees during the working hours. Those can be categorized into four major categories namely extra organizational, organizational, group and Individual stressors (Luthans, 2008).

2.6.1 Extra Organizational Stressors
It is a known fact that any organization is greatly affected by the external environment; therefore, it is clear that job stress is not limited just to the things that happen inside the organization, during working hours. Extra organization stressors include factors such as social/technological change, globalization, the family, relocation, economic and financial conditions, race and gender, and residential or community conditions.

2.6.2 Organizational Stressors
There are potential stressors associated with organization itself, which may affect to job stress of its own employees. Although organization is made up of groups of individuals, there are also macro level dimensions, unique to the organization that contains potential stressors. These macro level dimensions can be categorized as administrative policies and strategies, organizational structure and design, organizational processes and working conditions.

2.6.3 Group Stressors
There is a tremendous influence from group stressors on employee behavior and it can be a potential source of job stress. The group stressors can be categorized as lack of group cohesiveness and lack of social support. It is very clear that cohesiveness or togetherness is very important to employees; further employees are greatly affected by the support of one or more members of cohesive group. If there is no support or cohesiveness, work related stress may be increased in any organization.
2.6.4 Individual Stressors

All the stressors discussed above eventually get down to the individual level. Individual stressors may differ from employee to employee depending on the type of personality of the employees (Luthans, 2008).

2.7 IS POLICY AND JOB STRESS

Considering all the facts, which were discussed about the Information Security Policies and job stress, now it is the time to have an understanding how the impacts of Information Security Policies may affect the job stress of the employees through the literature.

Policy can be defined as broad guideline for decision-making that links the formulation of strategy with its implementation. Organizations use policies to make sure that, employees throughout the firm make decisions and take actions that support corporate mission, Objectives, and strategies. Information Security Policy comes under those corporate policies laid by the company (Wheelen and Hunger 2007, p13). Information security has become a vital role in today’s fast moving technically changing business environment. Therefore, organizations are taking each action to prevent, their secret information disclosure to their competitors as well as to the outside world. Information Security Policies came to the business world to provide basis for information protecting process.

Information Security Policy is a plan, outlining what the company’s critical assets are and how they must be protected. Its main purpose is to provide staff with brief overview of the acceptable use of any of the information assets, as well as to explain what it deems as allowance and what is not, thus engaging them in securing the company critical systems (Danchev 2003).

Due to enforcement of Information Security Policy, employees are facing to many activities, which may violate their privacy. Most of the companies are monitoring their employee’s activities during the office time without even informing them. In a PC world online survey, most of the respondents agree that employer has the right to monitor but employees should be informed first (Building an Acceptable use policy 2003).
66% of respondents agreed that employer has the right to monitor their activities while 27% disagreed for the same. Larger number of respondents that is 94% agreed for being monitored if they are informed first and only 4% disagreed for the same. It shows a fact that employees do not have any issue if the monitoring is done in ethical way rather then doing it unethically (Building an Acceptable use policy 2003).

Information Security Policies may enforce restrictions on internet usage. This may have an impact of employee’s freedom at the same time high usage of internet usage may be a threat to organization’s information as well. Following figure 2.2 is an example for how organizations put restrictions on personal internet usage (Building an Acceptable use policy 2003).

According to the figure 2-2, most of the companies tend to restrict non-work use while allowing limited usage after office hours. Some of the companies allow internet usage without any restriction at anytime where as very few companies do not have any policy on restricting personal internet usage.
Job stress results from the interaction of the worker and the conditions of work. Researchers found that there are many factors affecting the job stress such as working environment, role conflict, and role ambiguity. Interpersonal conflicts, job future ambiguity, job control, employment opportunities, quantitative work load, variance in work load, responsibility for people, underutilization of abilities, cognitive demand, shift work etc (Murphy, 1995). Working environment of employees may change due to the restrictions enforced by Information Security Policy.

When employees are working under monitored and controlled environment, their job stress may increase. Working in a stress full mind may lead to job dissatisfaction. Aspects such as job stress or job dissatisfaction also comes under the responsibility of the management. When management tries to monitor and control their employees more and more, their job satisfaction may go down. Job dissatisfaction is related (among other things) to the question of motivation. This is a crucially significant factor regarding performance of employees and it may directly affect the performance of the organization (Roelofsen 2002).

Information Security Policies may become a burden for employees due to many factors such as mostly employees are not aware about enforced policy by their
company. Sometimes unawareness of IS policy may increase due to unavailability of enforced policy.

Security Survey on UK and USA based organizations by Ernst and Young (1995), it was found that Thirty-seven per cent of UK respondents did not have a security policy, 65 per cent did not have a security orientation program for new employees (Figure 2.3), and (Figure 2.4) 56 per cent did not have an ongoing security awareness program for employees.

Figure 2-3 IS Security Orientation Program for New Employees

Figure 2-4 IS Security Awareness Programs
Organizations are responsible for making available their IS policy for employees to read and have a better understanding. Privacy violations by IS policy may be a hassle to employees if employees are not aware about their policy and if it is not properly enforced. Therefore, organizations need to pay special attention when implementing IS policy.

Implemented policy should be equal to the employees and employees should be educated about the effects of policy violations before enforcing punishments for policy violations. The Information Security Policy should be updated regularly and promptly and these updates should be circulated to all staff, affected by the policy (Kenneth, et al 2006).

According to the research, study carried out by Liyanagunawardena (2007), the presence of the Acceptable Use Policy in Sri Lankan Software organizations; does not make any significant difference in employee computer misuse. As per findings of the same study, increased awareness of Acceptable Use Policy has done make a positive influence on reducing employee computer misuse during office hours.

As discussed above there are lot of research studies were done in many contexts for finding factors affecting the job stress and how to manage the organization culture for implementing Information Security Policies. There is no any research done for Sri Lankan context to check whether the impacts of Information Security Policies are acting as job stressors. The Author is trying to do an empirical study to find out the relationship between the impact of IS policy and the job stress of the employees in Sri Lankan telecommunication sector.

2.8 SUMMARY

This chapter discussed about the concepts such as information, information security, and Information Security Policy and job stress. In detail, analysis on mentioned topics was given with support of literature. Latter part of the chapter directed to research topic, which is the impact of Information Security Policies on employee job stress. Literature related to the topic discussed in detail with references. Next chapter will discuss about the design of the research.