Shan Wu

REVIEW OF THE METHODS FOR THE DEVELOPMENT OF INFORMATION SECURITY POLICIES AT ORGANIZATIONS

UNIVERSITY OF JYVÄSKYLÄ
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS
2016

ABSTRACT

Wu, Shan
Reviews of the Methods for the Development of Information Security Policy at Organizations.
Jyväskylä: University of Jyväskylä, 2016, 70 p.
Service Innovation and Management, Master's Thesis
Supervisor: Siponen, Mikko

This thesis aims to have an overview of the current studies in the development of information security policy. The research is based on a systematical literature review. The study focuses on the development process of information security policy and other relevant issues in information security policy development within organizations. There are four research questions are proposed based on this topic: 1) what are the functions of information security policy; 2) what kind of stakeholders should be involved in the development of information security policy; 3) what is the information security policy lifecycle; 4) what are the methods in development of information security policy.

The research references were gathered based on a literature research searching strategy. There are eighty-three reference gathered include scientific papers, company documents, and actual information security policy documents used in organizations. A conceptual analyze in multiple dimensions is accomplished to answer the research questions. Key conceptual descriptions with similar opinions are gathered together for further processed.

The study summarized eight general functions which all the information security policy should achieve within an organization: represent the security strategy, plan the security requirements, define roles and responsibilities, define rules and protocols, state punishment, reduce risk, assist decision making, and provide the secured environment. Nine stakeholders should be involved in information security policy development phases: the user community, executive management, legal& regulatory, the ICT specialist, security specialists, human resources, business unit representatives, public unit representatives, public relations, and external representatives. A key outcome of this thesis is an integrated information security policy development lifecycle from twenty-nine development suggestions from different articles. According to the material analyzing, there are five development stages in information security policy development: formulate a security group, assessment, plan, deliver, and operate. Another essential contribution of this thesis is that the research gaps which should be fulfilled but missing in current research are pointed out for the future study.

Keywords: information security policy; development methods; development lifecycle; functions of information security policy; stakeholders of information security policy

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

The “information revolution” provides a significant impact on all forms of human life. Especially with the quick spread of Information Technology in business running; the “revolution” has altered the way people think and behave compared to how they used to be in the working domain. Information communication technology and service have optimized the modern business operation model. With the rising rate of ICT related investment, information is now considered an essential resource in organizational assets. Emails and other chatting tools have increased the efficiency of communication. Enterprise Resource Planning systems optimize the substance assignment and product chain. Additionally, with a powerful calculation and simulation capability, ICT products reduce the waste and abuse of all enterprise resources includes solid resources, human resource, and information resource while doing business.

There is no doubt that ICT assets produce opportunities and innovation, as well as new strategies. ICT services promote efficiency and quality of organizational services and products. However, the risk is embedded with opportunities. Information security should always be the priority concern in organizations since currently, information leakage is much easier and more harmful than it used to be. Information security has already be the priority concern in organizational strategy.

The definition of Information security, according to the book Information Security (Edition 3.0), is the practical behaviors which ensuring information is only processed (read, heard, changed, broadcast and etc.) by authorized people. (Information Security, Edition 3) The key point behind information security is protecting the information from unauthorized access. It considers information security as a protecting process rather than an application of a single defense tool such as the firewall. From an organizational perspective, information security is a management issue. Therefore, it requires management approach to achieve its goal.

Information security policy is one of the important controls needed within an organization to ensure the effective of information security and to achieve the implementation of information security management. It is a common choice for organizations to represent their security strategy. Information security policy is a document which declares in writing how an organization designs to protect the physical and ICT assets owned by the organization. Generally, an information security policy contains components like purposes, aims and commitments, responsibilities, risk assessment and classification of information, protection methods, compliance, and etc. Thus, the development of information security policy is an issue faced by most of the security specialists within organizations.

1.1 Background of the Thesis

1.1.1 Information Security Management

Information has proved its value by adding value to organizational products and services, reducing costs, and reaching the demand of customers. Considering the important role of information acts in modern business, information security becomes an essential component in organizational planning and management. More than one IS security researchers point out that information security is mainly a management and business matter rather than a technical problem. (Dhillon and Backhouse, 2002; von Solms and von Solms, 2004) Investment (a survey provided by Information Security Magazine, 2004) shows that information could not be secured only by security products or technology but also by a good management and implementation plan. The plan focuses on economic, risk and financial management as well as the implementation of IS security systems.

A common misunderstanding of information security in an organization is that it aims to protect the confidential of information. Protection of information resources is not that difficult, however, the objective of information security in an organization is protecting the business. Based on the definition of company objectives in the business dictionary, the purpose of organization usually focuses on its long range intentions for operating and its overall business philosophy. All organizational actions, employees, and assets are gathering in order to support the continuous of business. The objective of information security management is no difference.

Information security management could be defined as the protection of information security via a series of management activities. The contents of information security management are different according to the understanding of different researchers. Tudor (2001) suggested five components of information security architecture which are: security organization and infrastructure; security policy, standards, and procedures; security baselines and risk assessments; security awareness and training programs; and compliance. ISO/ IEC 17799 have a different explanation on scope of information security management. There are nine components of information security management provided by

ISO/ IEC 17799: security policy establishment and assessment; security organization and responsibility; personnel management and training; computer system security management; network security management; system access control; system development and maintenance management; information assets security management; physical and environment security management; and business planning and management.

Von Solms and von Solms (2004) noticed ten factors about information security management and they are listed below:

- Information security is a corporate management responsibility
- Information security is a business matter rather than a technical matter.
- Information security management is a multi-dimensional discipline
- Information security plan starts with assessment of security risks
- International security standards play an important role in information security management
- Information security policy is a key success factor in information security management
- A decent information security management structure is key success factor in information security management
- Information security management could not achieve its goals without monitoring and compliance
- The priority of information security management is the security awareness training
- The responsibilities of information security managers are supported by authorized infrastructure, tools and mechanisms.

1.1.2 Information Security Policy

An essential part of information security management is information security policy. An effective information security policy has been considered as the foundation of information security management. The definition of information security is varied from different researchers. The information Technology Security Evaluation Criteria (ITSEC) determines a corporate security policy as:

> The set of laws, rules, and practices that regulate how assets including sensitive information are managed, protected, and distributed within a user organization.

The definition of an organizational security policy is:

> The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes resources to achieve specified security policy objectives. These laws, rules and practices must identify criteria for according individuals authority, and may specify conditions under which individuals are permitted to exercise their authority. To be meaningful, these laws, rules, and practices must provide individuals reasonable ability to determine whether their actions violate or comply with the policy.

Another definition of information security policy provided by Rees, Bandyopadhyay and Spafford is:

> A method by which a well-defined process is put into place so that all the requirements of dealing with information security are considered in a foolproof manner.

Gaston (1996) suggests the definition of information security is:

> The broad guiding statements of goals to be achieved with regard to the security of corporate information resources.

Despite the various definitions, the aim of information security policy is similar. The purpose of information security policy is to give guidance about how information security is management in an organization. To users, it is a code of IT related behaviors in daily work. To junior managers, it is a management manual of information security. To the top managers, information security policy is the entity of representing the organizational security strategy.

The organizational document of Control Data (White Paper, 1999) points out there is three natural weakness of information security policy. These natural weaknesses are major courses of information security policies failure. Firstly, security is the obstacle to development. It is human nature to obtain more information with higher access right and faster response. Security management methods, even mild ones, reduce the organizational productivity. Secondly, information security is long-term learning progress rather than instinctual behavior. Therefore information security policy needs the user awareness training program to support. Thirdly, information security policy is an on-going project rather than a one-time thing. Preparation, planning, and practice levels the security protection skills up and reduce the faults and loopholes.

1.2 Motivation of the Thesis

Since information security policy is such a significant fundamental layer of information security management within organizations. It is worthy to study the relevant issues about information security policy. This Master's thesis studies the experiences and best practices related to information security policy development.

The purpose of this thesis is to invest the current studies on information security policy based on a conceptual review and determine the current methods in the development of information security policy. Firstly, I proposed four research questions about information security policy. Secondly, a series of reference should be determined and categorized. Thirdly, useful reference should be analyzed to answer the research questions. Finally, a discussion about the current situation on the research of information security policy would be announced, with the suggestion of future studies on this domain.

In this thesis, there are four research questions should be answered: 1) what are the functions of information security policy; 2) what kind of stakeholders should be involved in the development of information security policy; 3) what is the information security policy lifecycle; 4) what are the methods in development of information security policy.

In the end of this research, this thesis aims to increase audiences' understanding about the definition of information security policy and its functions. An integrated information security policy development lifecycle will be formulated. This thesis will also provide an investigative document about current methods in the development of information security policy with suggested stakeholders. Based on this thesis, a clear view of current studies on information security policy will be presented. This review study help pointing out the research gaps which should be fulfilled in this domain.

2 SYSTEMATIC LITEATURE REVIEW

This section offers an overview of systematical literature review and the research methodology of the conceptual review used in this thesis. It explains the definition and purpose of review based research.

2.1 Literature Reviews

A literature review is an important feature in any academic research. It simply summarizes the existing study about a research topic. A literature review is a secondary resource based which describes what other researchers have written on this subject. Wester and Watson (2002) indicates that an effective review states a solid foundation for academic knowledge. The objective of literature review defined by MISQ is aimed to:

> …promote MIS research by publishing articles that conceptualize research areas and survey and synthesize prior research. These articles will provide important input in setting directions for future research.

There are five steps for writing a review article based on the study of Webster and Watson (2002). Firstly, there are three steps to begin a literature review: introduce the topic and the motivation, define the key variables, and set the boundaries on the work. The second step to write a literature review is to identify the relevant references. The key success factor of a review article is fully focused on materials. Webster and Watson (2002) suggest a structured approach to search the relevant materials: 1) the leading journals are the major provider for the major contributions; 2) the reference lists of the leading journals could be the prior articles; 3) relevant articles could also be identified from the scientific digital libraries and the search engines. The third step for a literature review is to structure the review. Unorganized materials could not provide any new value. A literature review should be based on a structured review. There are two effective approaches: concept-centric and author-centric. The fourth step for a review based article is theoretical development. The forms of the development include (but not limit) models, propositions, and justifications. The theoretical development will identify the knowledge gaps and thereby encourage future researchers to continue this breach. The fifth step is to evaluate the theory. Berm (1995) points out that colleagues' review before submitting is one way to evaluate your theory. However, evaluating is still difficult to achieve. The last step for a literature review is to create the discussion and conclusions.

The key value of a literature review is to point out the essential issues which are missing in the study domain. A reviewed based research studies what have already done and what is missing about the research topic. The missing puzzle will lead the future research in this research topic.

According to the study by Webster and Watson (2002), an ideal review based article should:

- Motivate the research topic and explain the review's contributions
- Describe the key concepts
- Delineate the boundaries of the research
- Review relevant prior literature in IS and related areas
- Develop a model to guide future research
- Justify propositions by presenting theoretical explanations, past empirical findings, and practical examples
- Present concluding implications for researchers and managers.

2.2 Search Strategy

In order to search for available references, I have focused my research on search engines like Google (scholar.google.fi) and scientific digital libraries such as ScienceDirect and IEEE. There are also online documents from security companies which provide relevant information about information security policy. My searching behavior is mainly focused on the professional and scientific online-libraries; however, it could not ignore the value of organizational documents such as London University policy or SANS security company documents.

Figure 1 shows the search strategy of the useful reference I used in my thesis. This figure is a modification of the search strategy process provided by Unterkalmsteiner and his colleagues (2012) for the identification of papers. This flowchart shows the searching phases to determine the relevant reference. Furthermore, it also includes the checking phase to identify its relativity and validity.

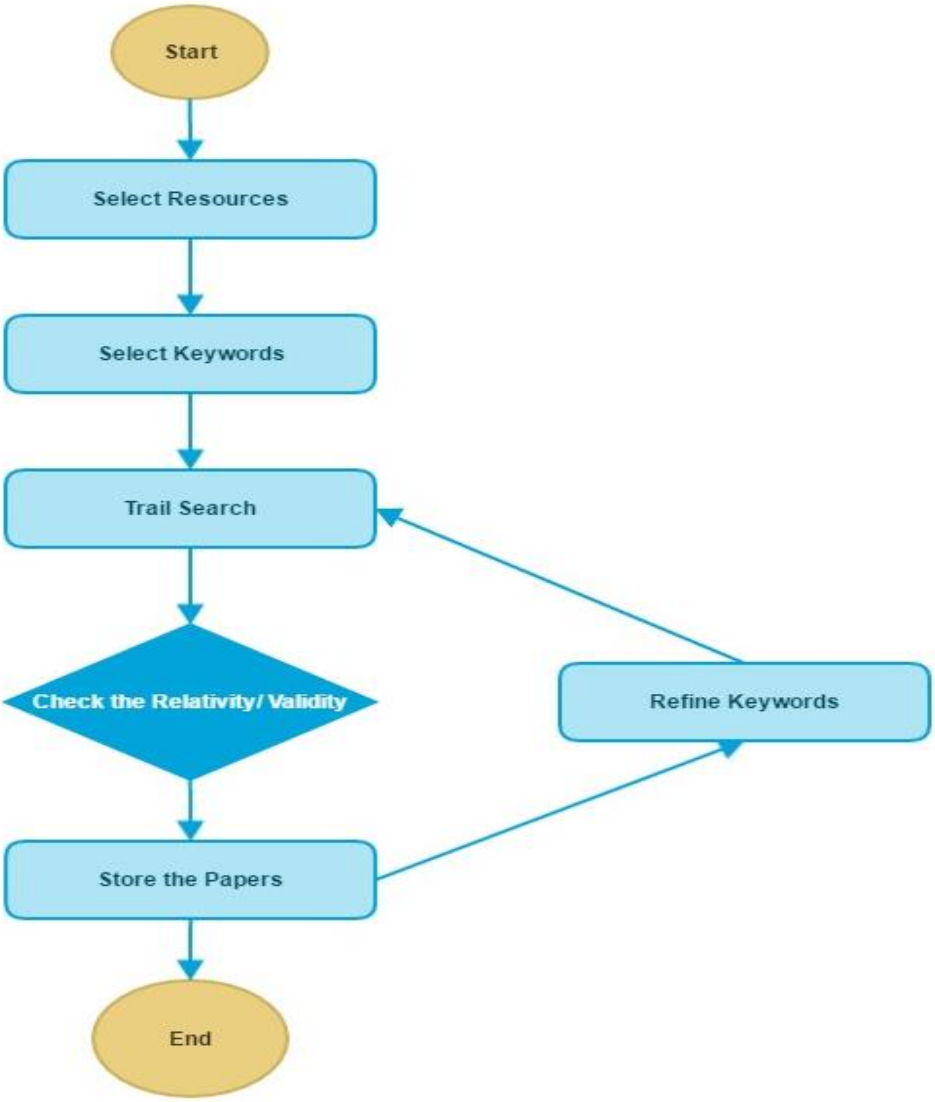


Figure 1: Search Strategy

For the research purpose, I seek for the available references by key strings such as “information security policy”, “security policy”, and added strings such as “in organization”, “security management.” After gathering several scientific articles, I tried to dig more useful references from the reference lists of the articles I had found. The reference lists of the previous articles show the value of those references which are proved by the authors. I contained those references in my literature review, either. It could be clearly identified that some articles are quoted more than once in several articles by different authors. (e.g.: “Information Security Policy – What International Information Security Standards say”)

I would quickly review the abstracts and findings of every article to check the relativity and validity. Since information security policy is an essential part of information security management, some information security management oriented paper will also mention information security policy. However, this kind of papers would not offer views with enough value under those research questions. Thus I skipped these papers which have less relevant information, only store the papers which their subjects are fully focused on information security policy. Finally, there are eighty-three articles are picked as the main research reference of this reviewed based thesis.

2.3 Analyze Strategy

All eighty-three articles are categorized by its publication source in Table 1. The main topic of all the articles is information security policy: its functions, its development methods, its lifecycle, its scope and etc. In order to study the relevant issues about information security policy in organizations, a research analysis based on literature review is accomplished.

Table 1: Publishers of the Articles

Literature publishers	**Numbers of articles**
A publication of EDUCAUSE	1
Business Computing	1
Computer & Security	11
Emerald Insight	1
IEEE	2
Information & Management	1
Information Management & Computer Security	5
Information Security Conference	7
Information Security Policy	1
Information System Security	3
Information Systems Journal	1
International Journal of Information Management	1
International Journal of Medical Informatics	1
ISSAI 5310	1
Journal of Information Technology & Politics	1
Journal of the Association for Information Systems	1
Logistics information management	1
Medical informatics and the internet in medicine	1
National Computer Board	1
None resources	17
Organizational document	22
Security management practices	1
The office of management and enterprise service information services	1
Total articles	83

There is a content analyze about information security policy functions. All the sentences, descriptions or paragraphs about information security policy's purposes or definitions were gathered for answering this research question. I put the similar views together with their authors and year. It assisted in the generalization of consensus from different researchers. The functions of information security policy are stated in Chapter 3.

For determine the methods in the development of information security policy, I did my contextual review research in this order. First of all, I formulated a table to list the articles by their authors, titles, published years, and abstract of this article. This would give an overall picture of what has to be reviewed. Secondly, I collected all the development phases mentioned in the articles to build an integrated information security policy development lifecycle. The development lifecycle and development phases are analyzed in detailed in Chapter 5. Thirdly, all articles which provided developing phases of information security policy, I searched the research methods applied in these articles. The research methods were collected and explained in Chapter 7.

3 FUNCTION OF INFORMATION SECURITY POLICY

More than one author emphasize that the foundation of organizations' information security management is an effective information security policy (Parker, 1998; Perry, 1985; Schweitzer, 1982; Warman, 1992). Every author emphasizes the capability of information security policy to explain its importance in information security management. However, they have different views and sayings about what an information security policy could achieve. The diversity of understanding in the functions of information security policy is caused by its variety objectives. The functions of one security policy in an industry factory are obviously different with a security policy in an educational institute. Different expectations in security management lead to different functions.

Despite the variety functions described by different authors, the explanation of information security policy functions is an essential section in a policy document. The function description section formulates the limit lines of this security policy document by policy writers. The limit lines will help policy writers accomplish their jobs better. In the meantime, information security policy function section also explains the objective and capability of this policy document to who this security policy document applied to. This section will help employees understand the policy in order to increase their security awareness. Furthermore, it will help them follow the security behavior guidance based on the security policy in the organization.

In order to generalize the functions of information security policy, I extracted all the descriptions about purposes and capabilities of information security policy. I gathered the sentences which discuss similar points and eliminate the divergence. Based on the excerpts, eight functions were summarized. These eight functions represent the major demands of information security management which are expected from an information security policy. They are also the main reasons why an organization needs the existence of information security policy.

3.1 Represent the Security Strategy

Most of the articles mentioned that information security policy represents the security strategy of the organization. The authors use different forms to describe the organizational security strategy include (but not limit): the security objectives, the objective of information security, security goals, statement of security management, and etc. Danchev (2003) points out that setting a company's security foundation is the main reason for an organization to develop an information security policy. According to Corpuz (2011), information security policy offers a security direction for organizations to implement their information security management. Galletta and Hufnagel (1992) point out, based on the definition of policy, a security policy refers to an organization's plan or strategy which defines its overall security goals and objectives. SANS security document suggests that a well-designed information security policy is able to define the objectives of the information system of an organization and outline a strategy to achieve these announced objectives. According to ISO 17799 international security standard, "information security policy provides management direction and support for information security". An effective information security policy, mentioned by Hone and Eloff, assists in achieving the information security objectives of the organization.

Information security policy is the most intuitive reflection of information security management of an organization. For the management point of view, information security policy is an announcement of organizational security strategy. Senior management of an organization will implant the security strategy in the process of developing information security policy. Meanwhile, a well-designed information security policy is a detailed guidebook leading the employees to achieve the security goals of the organization.

For the purpose of representing the organizational security strategy, the policy making group should have an accurate comprehension about the security goals of the organization. Generally security goals are determined by the executive management group and the security specialists. Security specialists could provide the professional security knowledge to assist the executive management personnel or team to integrate security strategy. Commonly, the security strategies should protect the security of information assets in the meantime guarantee the productivity.

3.2 Plan the Security Requirements

Information security policy proposes a plan of security requirements. Information security policy documents often contain the purpose, scope, constraints and applicability of information security policy .Tang (2003) points out that the objectives of the information security policy are to plan the security requirements and to form consensus in an organization. According to Baskerville and

Siponen (2002), a security policy acts as an overall plan in organizations which aims to cover the security goals as well as acceptable procedures. Danchev (2003) indicates that the security policy is a plan which pointing out the critical assets within organizations and the methods to protect them. Based on the report provided by National Computer Board Mauritius (2011), information security policy outlines the organizational baseline on security.

The nature of policy is a plan. Information security policy is a security plan within organizations. Information security policy plans what should be protected and how to protect. Based on the definition of plan, information security policy will give the structured process to achieve the objective, in this situation, the security goals of an organization. Information security policy will contain tasks and sub-tasks which should be followed in an order. Planning is time-saving and assists rational allocation of resources. Information security policy as a plan in security management makes an appropriate arrangement on limited resources and personnel to protect the most valuable and vulnerable information assets. In order to achieve a succeed plan, the executive management group, human resources, ICT specialists and security specialists should gather together to allocate the resource, both physical/information property and human.

3.3 Define Roles and Responsibilities

Information security policy defines roles and responsibilities of organization staffs when dealing with information. Galletta and Hufnagel (1992) point out that information security policy identifies not only the responsibilities of IT staffs but also the responsibilities of users. Lindup (1995) indicates that information security policy determines the signatories' rights and responsibilities. Eloff (1998) suggests that information security policy defines the responsibilities of all involvement parties. Whitman (2004) points out that information security policy defines individual responsibility and determines the authorized and unauthorized use of the systems. According to the report of National Computer Board Mauritius (2011), information security policy authorizes security personnel to monitor, probe, and investigate. Based on the study of Whitty (2010), information security policy ensures that every employee had a clear understanding of their responsibilities in protecting the information. Written in SANS security document, information security demonstrates each employee how he or she could contribute in maintain the security environment by fulfilling their responsibilities.

Information security policy clarifies the role and responsibilities of each employee. This is based on employee's security knowledge and their working domain. In this security document, written authorities are given to individuals who are in charge. Well-defined roles and responsibilities provide clear understanding about who is in charge and what to do. Authorized personnel has the responsibilities to guarantee the safety of information they handled and the system they used. Information security policy also points out the roles of every employee should fulfill to achieve the security strategy. The roles include monitoring, probe, investigation, and etc. For example, a security specialist could be authorized to monitor the daily IT behavior. His or her responsibility is to check the system and determine the unauthorized behavior. It is also his/her job to report the unauthorized or unappropriated behavior to a senior management. It is the senior management's responsibility to decide the punishment.

3.4 Define Rules and protocols

Information security policy defines rules and protocols. The TCSEC states that the definition of information security policy is the minimal set of laws, rules and practices about how to manage and distribute sensitive information within organizations. According to the report provided by National Computer Board Mauritius (2011), information security policy stipulates the rules for expected behavior by all stakeholders including end users, security personnel, ICT experts, and etc. Hu suggests that security policies also determine a series of rules to supervise provided applications and services by their domains. Written in SANS security document, information security policy should be a central document that describes authorized behaviors in details with scope and applicability. Ward and Smith (2002) point out that information security policy provides security controls and protocols for guarantee the security of information system security.

Rules and protocols defining is an important section in information security policy. It is a guidebook of security behaviors. Unlike roles and responsibilities, rules and protocols provided by information security policy are more focus on the behavior itself rather than the personnel. Information security policy gives clear guidance to its signatories about how to protect sensitive information steps by steps. For example, information security policy about email will state that "please log out your email when you are leaving your computer". It is a rule for employees to obey and whoever violates it should be punished. Based on the standards and protocols provided by information security policy, it is convenient and easy for all stakeholders to fulfill their responsibilities.

3.5 State Punishment

Information security policy also states the punishment for unauthorized use. According to the report of National Computer Board Mauritius (2011), information security policy determines and authorizes the consequences of violation. Whitman (2004) points out that penalty for violations are defined by information security policy. Written by SANS security document, information security policy should include the penalty for misuse.

Punishment is one of the key sections in information security policy. Punishment has a tight connection with responsibilities and standards. When the authorization is given and the rules are set, all behaviors which are against it should be punished. A reasonable punishment is one of the driven enforcement for all stakeholders to obey the policy. Information security policy could not achieve the security goals without punishments Punishment stated in the policy document includes (but not limited) amercing, demoting, interdicting, and firing. The degree of punishment is depending on the consequence caused by unauthorized behavior and how sensitive the information is. Information security policy which declares the punishment is a warning for employees to understand the consequence of ignoring the policy. It is also an instruction for senior management to react after unauthorized behavior.

3.6 Risk Reducing

Information security policy reduces risk. It is not only the direct purpose of information security policy, but also the plain requirements or the security requirement within organizations. Whitty (2010) points out that information security policy mitigates the risks as well as ensures the protection of all sensitive information. Written in SANS security document, information security policy could identify how incidents will be handled.

Identifying risks and preventing systems from potential threats are the basic capabilities of information security policy. It is also an early stage of development phase in information security policy development lifecycle. Without these, information security policy is valid to the organizations. Information security policy determines the potential risks and provides methods to avoid risks, eventually reach the purpose of reducing risks.

3.7 Assist Decision Making

Information security policy assists in decision making. Cresson (1996) points out that information security policy lead the product selection and development. According to RSA security document, information security policy force to make return-on-investment decisions. Also, it is written in SANS security document, information security policy balances the protection with productivities.

Information security policy could not only guarantee the security of the organization, it has the business value which aims to assist the decision making on product producing. After all, the top goal of information security policy is not ensuring the security of the system but guarantee the contingency of business. By achieving the security goal, information security policy assists top managers to make the right choice in order to extend the business in a secured environment. It balances the security from productivity. An obvious example is how information security policy could assist purchasing daily products. Having the assistance of information security policy, officers in the purchasing department would choose the most secured applications and services after considering the funding. All top management who has the responsibility to make decisions would consider security based on information security policy when making a selection. Information security policy is their strong support for security issues.

3.8 Provide Secured Environment

Information security policy offers a secure and safety working environment for all users, according to Whitty (2010). A secure working environment is necessary for employees to focus on their work and do not disturbed by unexpected threats. Information security policy involved all the stakeholders within organization to systematically build a secure environment for a healthier business operation process. It is a blueprint for building a secure environment for business. However, no scientific paper could provide the evidence to support this function.

Obviously, there are more existing functions of information security policy. These mentioned eight functions are the primary functions for general information security policies. Information security policy which has special purposes will have more functions than these eight. Such as information security policy for the military is also protect national security. These peculiar functions remain to the future research to generalize.

4 STAKEHOLDERS OF INFORMATION SECURITY POLICY DEVELOPMENT

During the development of information security policy, a series of stakeholders should be involved in the development phase. Maynard, Ruighaver, and Ahmad (2011) did a research based on literature review and contextual interview about which stakeholders should be involved in security policy development process.

Due to the contextual reviews, there are nine synonyms of stakeholder types are mentioned which are: executive management, business unit representatives, user community, human resources, ICT specialists, external representatives, legal and regulatory, security specialists, and public relations. Each stakeholder synonyms may involve in information security policy development, mentioned by Maynard, at different levels. Meanwhile, in every different organizational development stage, they may have different opinions and contributions about policy. Thus, all possible stakeholders should be considered in the development of information security policy. These nine synonyms will be explained in details to help decision makers have an overall view while planning to develop a security policy for an organization. Table 2 is the summary of nine synonyms of stakeholders which are provided by Maynard, Ruighaver, and Ahmad (2011).

Table 2: Stakeholders of Information Security Policy Development (Maynard, Ruighaver, and Ahmad, 2011)

Synonym	**Stakeholders**
Executive Management	Top Management (Abrams& Bailey 1995) Managers (Baaskerville 1988; Leinfuss 1996; Szuba 1998; Tudor 2001) Senior Management (Henderson 1996; State of Oregon 1998; Woodward 2000) Corporate (Robinson 1997)
Business Unit Representatives	Group Management (Warman 1992) Business Units (Anderson Consulting 1999) System Owner (Baskerville 1988; Swanson 1998)

	Resource Owner (Tudor 2001) Information Owner (Swanson 1998) Data Providers (Szuba 1998) Junior Management (Warman 1992)
User Community	End Users (Baskerville 1998; Warman 1992; Leinfuss 1996; Swanson 1998) Computer Users (Abrams & Bailey 1995) Data Entry Staff (Szuba 1998) Data Processor (Szuba 1998) Information Collectors (Szuba 1998) User Groups (Diver 2007)
Human Resources	Human Resources (Anderson Consulting 1999; Diver 2007)
ICT Specialists	Technical Computer Specialists (Warman 1992) System Designer (Baskerville 1988) IT People (Robinson 1997) System Administrator (Swanson 1998) IS Professionals (Anderson Consulting 1999) IT Department (Woodward 2000) Technical Writers (Diver 2007) Technical Personnel (Diver 2007)
External Representatives	External Consultants (Gritzalis 1997) Clients (Baskerville 1998)
Legal & Regulatory	Legal Department (Robison 1997) Legal Counsel (Szuba 1998; Diver 2007) Legal and Regulatory People (Anderson Consulting 1999) Industrial Standards and Professional Licensure (Baskerville 1988) “The State” (Baskerville 1988) Audit and compliance (Diver 2007)
Security Specialists	System Security Manager (Swanson 1998) Security People (Anderson Consulting 1999) Information Security Team (Diver 2007)
Public Relations	Public Relations (Anderson Consulting 1999)

4.1 The User Community

Since it is provided by more than one article that human is the weakest point in information security, information security policy is designed for human beings. Mentioned in the multifunction of information security policy, it is a guidebook for employees to follow. To achieve the purpose, user behavior and user understanding about information security should be studied. Thus, the user community should be a stakeholder involved in the development of information security policy.

The user community, often known as ‘end user‘, composed of individuals who execute a series of different functions. It could also be addressed in security reference as computer users, user community, data entry staff, data processors, and etc. (Maynard, et al 2011) Due to the fact that most of the security risks are caused, intentionally or not, by end users in the organizations, the user community should be involved in the development of information security policy. The other fact is that the end user is accounted for the largest proportion of who the information security policy applied. The necessary of the user community involvement is self-evident. As mentioned before, securing assets is a learning process. The development of information security policy continues after the policy written completed and published. User awareness training is an essential stage of information security policy lifecycle. Preaching the policy is a necessary process of information security management.

4.2 Legal & Regulatory

Business crime is unavoidable in every commercial organization especially large companies. Participants involved in business crime are not hesitating to break the laws to achieve their purpose, stealing the secured information for individual benefits. Despite the business crime, there are also other inappropriate activities in the eyes of senior managers within organizations. Because of those situations, companies included legal advance in their policy development teams to make sure their information security policy is the legal explanation.

The main duties of the organizational legal department are analysis of the legality of the organizational legal related risk management and control. The responsibilities include decision-making, contract management, personnel training, supervision, and compliance monitoring. The legal department should be a compass in dealing with legal issues. Thus, the legal department provides legal advices based on not only legal risks but also business strategy, organizational operation, as well as market changes. Since the legal department is an indispensable part in decision making within organizations, information security policy which as a representing of organizational security strategy should involve the legal department. The legal department could offer professional opinions on legal domain to guarantee the compliance of the policy document. Also, they are involving in policy violation judgment including litigation, arbitration, reviewing, and mediation.

4.3 The ICT Specialist

Nowadays, information is transmitted mainly through ICT services. ICT services in the front line for protect the security of information. And the concept of information security should be embedded in the design theory of ICT services. Due to this fact, the ICT specialist with their professional background should understand how to protect the information transmitted via ICT service. They normally act as one of the main driving forces of the information security policy development.

The main jobs of ICT department are network management; information management; e-commercial planning; ICT-related employees training; technical updating; and assisting ICT-related issues. Their roles contain technical computer specialist, the system designer, ICT specialists, the system administrator, and etc. (Maynard, et al 2011) ICT specialists play an essential role in informatization within organizations. Thus, information security could not achieve without ICT specialists. The involvement of ICT specialist in developing process is based on their technical knowledge on system design and security knowledge of those systems. They know the best about the weak point and loophole in ICT systems. This knowledge comes from their experience in building and maintaining the computing infrastructure within an organization. It is also their responsibility to involve in user awareness training.

4.4 Security Specialists

The security specialists in the organization are employed personals who focus on protecting organizational information, and on the development of security policies. Most of the Security Specialists are preview ICT specialists, however, change their career from designing and development of ICT systems to protection of information security. Thus, the security specialists possess the understanding in both ICT product and service innovation and security concerns.

Based on the review, the security specialists should be the leading role in the development of information security policy. The security specialists explain the importance of information security to the executive management to start the development of information security policy. During the design and development phases, the security specialists offer their knowledge in protection in order to develop an effective security policy. Moreover, the security specialists assist in design user awareness training program.

4.5 Human Resources

Information security policy defines roles and responsibilities for each participant. It is the responsibility of human resources department to help insist this defining behavior with the security team. Human resources involvement is most important to ensure that policy meets the requirement of the organizational standard. Human resource department is responsible for human resource management within organizations. The main purpose of human resource department is providing and training qualified employees for the organization. Human resource is in charge with recruitment, performance management, training management, employee relations, and wages. Human resource department plays different roles in the different development stage of an organization; however, it is the major management of connecting and interaction between employees to accomplish the business objectives.

Anderson consulting (1999) suggests that human resources should be involved in the development phase to develop the communication plan and ensure the communication channel of information security policy. Their responsibility in developing information security policy includes (but not limit) changes to the job description, motivation, security awareness training and policy enforcement.

4.6 Executive Management

Since information security policy states the organizational security strategy and assists decision making, it is important to involve executive management in the development of information security. Kadam (2007) points out that involving senior management is a key success factor in developing and implementing information security policy. The original driving force, according to Woodward (2000), should come from senior management.

Executive management contains top management, senior management, and other managers. This group should support the development of information security policy on the management level. The executive management should be in charge of planning, implementing as well as allocating resources. It is also their responsibility to balance the information security with productivity. Executive management should define the priority task in information security policy. Based on the description, executive management should be involved in the development of information security policy from start to the end. Executive management should be fully in charge in every phase, formulating plans and delivering authorities to relevant individuals. Executive management is the leader of policy development team and adjusts development strategy based on current situation.

4.7 Business Unit Representatives

Business unit representatives are often defined as the ownership of systems and information. Tutor (2001) suggests that the resource owner should be involved in the developing phase of information security policy since they understand the importance of protecting the information. Swanson (1998) points out those information owners have the responsibility to ensure the effective of their information's security; therefore they should be involved in the information security policy development.

Despite the owners of information, other business units like junior management units, business units, or group management should be involved in the development of information security policy. Business unit understands the value of information, the benefit which is brought by information, and the loss which caused by information leakage and other relevant threats. This kind of acknowledges is from the daily experience of business. Business unit assists the development of information security policy by proving the business value of information assets and calculating the loss caused by information risks. Business unit explains the value of information to the end users better than ICT specialists because the explanation is based on their experiences. It is more persuasive and realistic for the business unit to show the damage of unsecured information.

4.8 Public Relations

Information security is not only a security thing in the organization. It is also a public relations issue. Organization would own their reputation if it is shown to the public that the organization is committed to security. Customers will increase the confident for the products and services provided by the organization if their information is secured. Thus, development of information security policy should involve public relations.

Public relations suggested by Anderson Consulting (1999) to be involved in the information security policy development process. Generally, there are three functions of public relation department within an organization. Public relation department promotes the achievement of corporate strategy, motivates product sales, and participates in decision-makings. Public relation department is a bright to connect customers with the organization. It is their responsibility to create a trust relationship between customers and the organization and to build a good corporate model. Therefore, it is public relations' responsibility to present the organizational security strategy, include information security policy, to the public.

4.9 External Representatives

With the unit of the business world, the value of information increases through sharing. Under this circumstance, it cannot shape the individual organization from cooperation in business while considering the information security issues. It is necessary to ensure the security of information which translated via strategic cooperation or supplier chain. The agreement should be reached among cooperation participants to achieve the security strategy of all. Due to this purpose, external representatives should be involved in the development phase of information security policy. For this cooperation behavior, it is more complicated to develop an information security policy than within the organization. It is not only because more participants are involved in, but also because information will be transmitted through the internet instead of the intranet. The information security is difficult to monitor and to supervise.

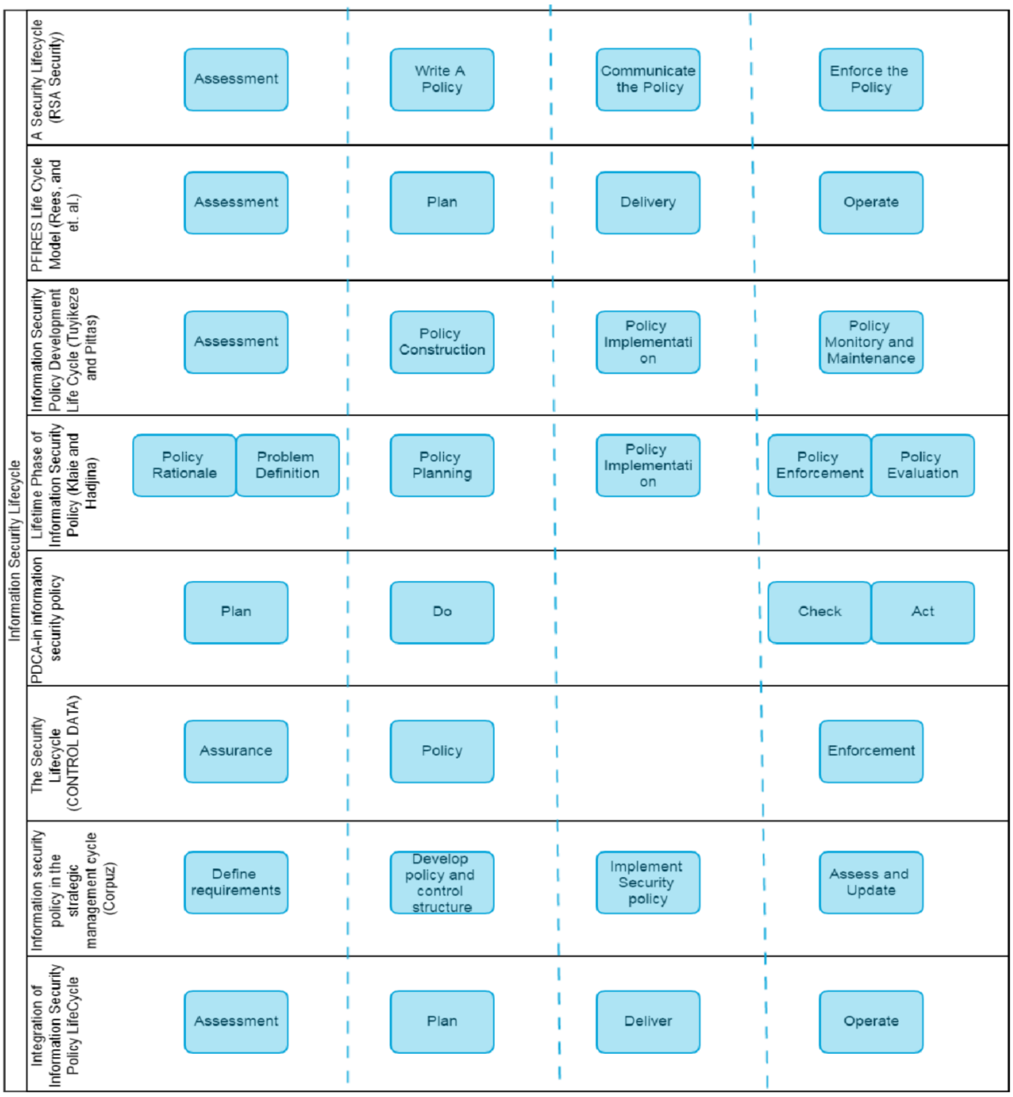
External representatives include (but not limited) customers, suppliers, external consultants and other external entities. Baskerville (1998) points out that it is also necessary to involve outside client who is relevant on organizational systems in the development of information security policy. Policy development involving external representatives will ensure the contingency of cooperation by secure the shared information. It should be followed by all stakeholders involved in the cooperation.

5 DEVELOPMENT PHASE ANALYSIS

There are more than one articles mentioned about lifecycle or lifetime phase of information security policy. It presents the phases or processes in the development of information security policy. The information security policy lifecycle gives a clear view of the preparation of policy creation to bringing of policy into the organizations. Development lifecycle of information security policy is guidance for the security team to create information security policy based on different organizational requirements. It is essential to study the similarity and differences of information security policy development phase.

To achieve the purpose of studying the commonality of difference information security policy lifecycle, an analyzed framework is created. This chapter presents the evolvement of an integrated information security policy lifecycle from previews studies. In the beginning, I summarized initial information security policy development phases from seven lifecycles providing by different authors. Based on these phases and some literature reviews, I tested all the development phases provided by the reference. This step is to check if there are missing phases provided by other articles than these seven lifecycles. In the end, an integrated information security policy development lifecycle was formulated.

Figure 2 is the first developing step of this section. Seven lifecycles or life phases of information security policy are listed below in Figure 2. Similar development stages are merged to one development phase. The last row integrates four processes of the lifecycles and names each phase.



Information Security Lifecycle

A Security Lifecycle (RSA Security)	Assessment	Write A Policy	Communicate the Policy	Enforce the Policy
PFIRES Life Cycle Model (Rees, and et. al.)	Assessment	Plan	Delivery	Operate
Information Security Policy Development Life Cycle (Tuyikeze and Pittas)	Assessment	Policy Construction	Policy Implementation	Policy Monitory and Maintenance
Lifetime Phase of Information Security Policy (Klaie and Hadjina)	Policy Rationale Problem Definition	Policy Planning	Policy Implementation	Policy Enforcement Policy Evaluation
PDCA-in information security policy	Plan	Do		Check Act
The Security Lifecycle (CONTROL DATA)	Assurance	Policy		Enforcement
Information security policy in the strategic management cycle (Corpuz)	Define requirements	Develop policy and control structure	Implement Security policy	Assess and Update
Integration of Information Security Policy LifeCycle	Assessment	Plan	Deliver	Operate

Figure 2: Analyze of Information Security Policy Lifecycle

Even though the phase of formulating a security team is not mentioned in any information security policy development, it is highly recommended in some articles (Doherty and Fulford, 2005; State of Oregon, 1998). As the result of this, I added the formulating a security team at the beginning of the information security lifecycle.

Adding with the development phase “formulating a security team”, five development phases become the phase analyzing of security policy in Table 3. Table 3 is the table to analyze the development phases. There are three columns in this table providing relevant information. The first column is the author who provides the development phases. The second column is the main analyze of phases of security policy development. Since PFIRES Lifecycle model (Rees, Bandyopadhyay, and Spafford) provides a clear and logic sub-tasks under each development phase, I use these sub-tasks instead of generalizing from the reference. The last column is the criteria whether the phases should be followed in an order or not.

Table 3: Analyze of development phases under Information Security Policy Lifecycle

Authors	**Phase of security policy**									**In order or not**
	Formulate a security group	**Assessment**		**Plan**		**Deliver**		**Operate**		
		Policy assessment	Risk assessment	Policy development	Requirement definition	Control definition	Controls implementation	Monitor operations	Review trend and manage	
Gritzalis, 1997			Answer a series of baseline generic question	Security principles Security guidelines				Deontology code		Yes
RSA Security			Assess security requirements	Write the security policy			Implement the security policy Communicate enforce		Implement the security policy reassess the policy	Yes
Lindup, 1995			The problem addressed by the treaty	Defines rules and protocols	Clarify the rights and responsibilities			The processes for verifying compliance		No

			The scope of the treaty					Sanctions		
Kabay, 1996			Proceduere1: To assess and persuade top management	Proceduere3: to form and draft a policy	Proceduere2:To analyze information security requirements		Proceduere4: to implement the policy	Proceduere5: to maintain the policy		Yes
Rees et, al		Policy assessment	Risk assessment	Policy development	Requirement definition	Control definition	Control implementation	Monitor operating	Review trends and operation management	Yes
Baskerville and Siponen, 2002				Design process: -creation of policy and sub-policies hierarch	Design process: -adjusting the levels of abstraction and enforcement needed		Implementation: testing			Yes
Doherty and Fulford, 2005	Step1. Assemble strategy team		Step2. Conduct situation analysis	Step3. Formulate strategy: create/ modify information security policy			Step4. Implement strategy: review/ modify information strategy		Step5. Review strategy	Yes

Tuyikeze and Pottas, 2010			Risk assessment	Policy construction			Policy implementation	Policy monitoring and maintenance		Yes
Danchev, 2003		Step3. Security policy violation	Step1. Risk analysis		Setp2.Risk management		Step4.The implementation of policy			Yes
Computer technology research group, 1998			1. Determine what assets need protection 2. Determine the level of protects for each assets 3. Determine internet usage 4. Determine the threats that exists 5. Explore how to address the threats 6. Conduct an impact	7. Draft a security policy		8. Add a recovery section in the plan		9. User training 10. Respond to incidents		Yes

			assessment							
Walton, 2002	Origination phase		Assessment of the current environment	Defining the security standards		Security architecture development			Migration planning and integration	Yes
Lee, 2001, SANS					Defines the objectives of the IS of an organization and outlines a strategy to achieve stated objectives	Construct the policy to reflect the corporate culture		Inform and educate the organizations		Yes
Anderson				Security policy development			Protection mechanism	Standards		Yes
State of Oregon, 1998	Develop a working group			Brainstorm and develop policy points for review				Once finalized, get top management endorsement Brief employees and gain signatures from them		Yes

DTI, 1999		Research policy content		Draft policy				Obtain management approval Issues policy to staff Monitor and maintain		Yes
MoConnel, 2000-2002, SANS				Security policy development: 13 tips				Security policy assessment and enforcement		No need to be in order for tips
Hagen, et al, 2008				Security policy				Procedures and controls Tools and methods Awareness creation		yes
Olnes, 1994			Step1. Survey for requirements: Resources/ threats and risks/ special goals	Step3. Implementation of security measures: responsibilities and documentation	Step2. Selection of countermeasures:			Ste4. Maintenance and daily operation: change in resources/ organizational changes/ security revision		Yes

Talbot and Woodward, 2009	Step1. Create an ITC education program Step2. Create an ICT security policy awareness program	Step3. Review existing policy		Step4. Rewrite existing policy				Step4. Improve policy enforcement Step5. Establish policy compliance checking and reporting Step6. Establish non-compliance report		YES
Cosic and Boban, 2010				Plan		Do		Check	Act	YES
Kadam, 2007			Step1. Threat identification Step2. Vulnerability assessment	Step4. Writing information security policy	Step3. Identifying action plans	Step4. Writing procedures and guidelines		Step5. Implementation: top/operations/ everyone		Yes
Knapp, et, al., 2009			Risk assessment	Policy development			Policy approval	Policy awareness& training Policy implementation Policy enforcement	Policy review Policy retirement	Yes

Canavan and Diver, 2007, SANS	Determine a compliance grace period	Review existing policy	Determine research materials Interview SMEs	Write initial draft Style considerations	Review cycles Review with additional stakeholders	Policy gap identification process Develop communication strategy Publish	Active communication strategy	Regular review and update		Yes
National computer board Mauritius, 2011	Policy development team			Development approach				Introduction of the policy to employees Positive operation of the policy	Policy assessment and review	Yes
Woodward, 2000			Study risk	Formulate policy	Develop standards			Get co-operation from management	Review	Yes
Ward and Smith, 2002	Project initiation			Security policy development		Consultation and approval	Disseminate policy	Security awareness and policy education		Yes
Corpus			Step1. Determine enterprise security requirements	Step2. Develop security policy and control structure			Step3. Implementation security poicy	Step4. Assess and update policy according to evolving business requirements		Yes
Hone and Eloff				Development		Presentation	Commitment	Dissemination Maintenance Styling		Yes

Wood, CISA, CISSP, 1995			Gathering key reference materials	Defining a framework for policies		Preparing a coverage matrix				Yes

Based on Table 3, all the development phases provided from the relevant articles could fit into these five development phases. It is safe to say that this five development phases could be formed to an information security policy development lifecycle. Figure 4 is the version of an integrated information security policy development lifecycle. More details about each develop phase are explained below.

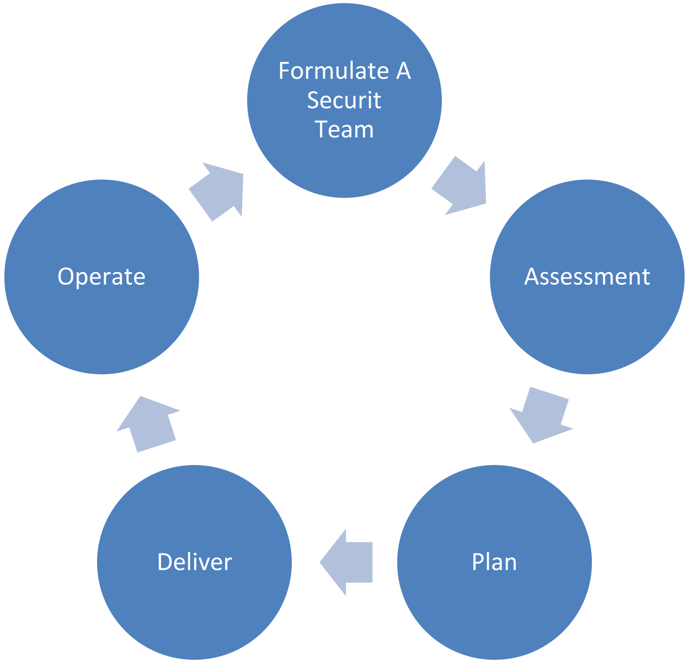


Figure 3: An integrated information security policy development lifecycle

5.1 Formulation of a Security Group

The first phase of information security policy development is the formulation of a security group. The security group is in charge with the following phases of policy development. All the tasks and subtasks are launched around this security group. The main responsibilities of a security group are to plan the development and react based on changes. It is also their job to deliver authorities and set roles to relevant individuals.

To formulate this response team, a group of relevant stakeholders in development of information security policy should be gathered. Usually, the security group contains the senior manager, the security specialists, ICT specialists and human resources. In some special case, the group also contains the legal& regulatory team, business units, and other relevant stakeholders. Members in this security group might have different roles in information security policy development due to their variable capability and professional knowledge.

5.2 The Assessment

The Assessment Phase is the second phase in security policy development. The Assessment Phase identifies the potential risks and reviews existing policies in the organization. The goal of the Assessment Phase is to evaluate the advance alteration against the environment and policies existed in the organization. The expected results of the assessment phase should be including an assessment of existing policies; an organizational assessment about current situation; a potential risk assessment; a policy development plan; and a communication plan.

There are two steps to accomplish the Assessment Phase: policy assessment and risk assessment. Policy assessment aims to determine the current situation about organizational policies through assessing the existing policies and relevant documents such as standards, guidelines, and procedures. If this is the first time for the organization to develop an information security policy, this policy assessment could be replaced by definition strategic. Risk assessment defines the business assets which the organization what to protect, and determines the potential risks embedded under those assets. Risk assessment document aims to help the security group to make decisions whether to continue information security policy development by moving to the next phase or not. There are four sub-tasks suggested by PFIRES (Rees, Bandyopadhyay, and Spafford) in the risk assessment: identify the assets, identify vulnerabilities, summarize risk assessment results, and evaluate possible measures and controls.

5.3 The Plan

The third phase, the Plan Phase contains the policy development and the requirement determination. The Plan Phase delivers the identification of current needs and strategy to change. The expected results of the planning phase should include the security strategy modified or updated from previews one; an updating or new policy; a requirement document about what should be changed; and in the meantime the execution of the communication plan. In the end of the Plan Phase, there should be a completed information security plan created for the organization.

There are two sub-steps under the Plan Phase which are policy development and requirements definition. Policy development aims to offer a new security policy and strategy based on the assessment phase. PFIRES (Rees, Bandyopadhyay, and Spafford) suggests two sub-tasks: create /update security strategy, and create/ update security policy. A security strategy is an overviewed direction for future business which under security controls. To create a security strategy contains tasks including determining security options; prioritizing security proposals and documenting the strategy. A security policy contains creation includes: identifying applied areas of security policy, drafting, reviewing, and publishing. On the other hand, the goal of requirements definition is to determine the requirements of the new security architecture based on the analyzing of organizational security policy. PFIRES (Rees, Bandyopadhyay and Spafford) suggests three sub-tasks: translate suggests to needs, exploit exhaustive security requirements, and confirm those requirements.

5.4 The Deliver

The fourth phase is the Deliver Phase which presents the situation after the complement of the policy. It presents the process to introduce the implemented policy document to daily security behavior. The expected results of the Deliver Phase include guidelines, procedures, standards and security controls for an implementation; and an enforcement plan for information security policy.

There are two tasks under this phase which are control definition and controls implementation. The control definition refers to all the relevant processes that reduce the risks. This step determines the compatibility between controls and d the requirements of information security policy. PFIRES (Rees, Bandyopadhyay, and Spafford) suggests four sub-tasks under the controls definition steps: design infrastructure, determine controls, evaluate solutions, and select controls. Followed by the control definition is control implementation. The controls implementation contains four sub-tasks, suggested by PFIRES (Rees, Bandyopadhyay, and Spafford): create implementation plan; build; task; and pilot and development.

5.5 The Operate

The last phase of policy development is the Operate Phase. It presents the monitoring and controls of information security policy on a daily basis. It assists identifying the upcoming risks and security requirements which force the modification of information security policy. Moreover, business and technology trends are watched and analyzed.

There are two sub-tasks contained in the operate phase: monitor operations, and review trends& manage events. Monitor operations aim to identify the daily activities within the organization to ensure the security enforcement. There are five activates in monitor operation which are administration and operations, communications, security services, investigation, and compliance. The final sub-step of Operate Phase and the security development is review trends and manage events. This step aims to determine the signal which represents the security policy need to re-evaluate. PFIRES (Rees, Bandyopadhyay, and Spafford) suggests four sub-tasks: manage events; identify internal trends; identify external trends; and escalate to assess phase.

Based on these five phases, it is analyzed by all the processes or methods mentioned in the reference. All the processes mentioned could be fit into the phases and sub-steps. Also, most of the processes should be executed in order. Except for some tips under the subtasks such are using understandable words in the policy document, orders are the emphasis by authors in security policy development.

6 EXAMPLES OF EACH DEVELOPMENT PHASE

Based on the analyzing table, there are five phases in a development lifecycle of information security policy. To increase the further understanding of each phase, I picked a representative example in each development phase and give a detailed explanation in this section. Each example represents one suggestion for the author about what should be including in this phase.

- Formulating A Security Group

In the beginning of security policy development, a security group should be formulated. It is important to identify the involved stakeholders in development of information security policy. The security strategical team should be involved in the whole processes of information security development. The security team should be in charge with the overall responsibility for developing the policy document.

The National Computer Board (2011), for example, states two kinds of involvement in the phase of policy development team. It mentioned two kinds of involvement in policy development team. The primary involvement includes information security team and technical writer. The secondary involvement includes technical personnel, legal counsel, human resources, audit and compliance, and user groups. In this paper, it is emphasized that information security team is authorized to possess the overall responsibility for the policy documents' development. There should be one person in full control with others supporting.

- Assessment Phase

The second phase is the Assessment Phase. Two kinds of assessment are accomplished in this phase. In the policy assessment, if the company has any business policy or existing security policy, it is better to review the policy document. For example, Canavan and Diver (2007) point out that the policy assessment guarantees that development of new security policies will not be against the organizational business strategy. Meanwhile, the security team will have a general understanding of current company attitude on a given issue or technology. Existing guidelines or security policy could be the start point in policy document writing on the same domain.

In the risk assessment, Computer Technology Research Group (1998) as an example suggests six steps. Those six steps are: identify what information assets need to be protected, define the protecting level for each asset, identify internet usage, determine potential threats, investigate on how to deal with the threats, and deliver an impact assessment. The major goal of risk assessment is to identify the business assets the organization is willing to protect and the potential risks are hidden inside those assets.

- Plan Phase

The third phase is the Plan Phase. For instance, RSA security Inc. suggests that there are six domains should be involved in policy writing. A Cover letter in the beginning written by CEO aims to emphasis the importance of information security in the organization. The purpose section is an overview of security policy document to explain the goals of this policy document. The policy document also contains the responsibility and authority section. In this section, it will be defined clearly about stakeholders' responsibility for developing and enforcing the policy. Definitions of the technical terms should be included in security document for non-technical readers to reduce the misunderstanding. Information ownership and access rights are a general statement defining the ownership and statement rights for the information on the company or transmitted via the internet. At last, computer system usage section defines the primary purpose of organizational computer systems as being for organizational business purposes only. For the requirement definition sub-tasks, there is not a suitable example of guidelines for requirement definition; it remains for the future study to accomplish the gap.

- Delivery Phase

The fourth phase is the Delivery Phase. Even though there are two subtasks suggested in this phase, most of the development processes in the article are focus on the control implementation sub-task. For example, Canavan and Diver (2007) suggested a development of communication strategy, publish, and active communication plan in this phase.

The communication strategy is just one example in delivery phase which should be considered by the security team. It represents one delivery method of the policy document to the end-users. There are few suggestions provided by Canavan and Diver (2007), which are: make information security policy embedded in a contract, involve information security policy to a training course; and apply a subscription-based communication method. Organizational culture and protection mechanism should also in the consideration of delivery phase to develop and implement the control.

- Operation Phase

The fifth phase is the Operation Phase. One example is the study of Oregon (1998); there are three domains in maintenance and daily operation. These three domains are change in resources, organizational changes, and security revision. Since security is a lasting process, changes and improvement will cause the updates. Another example is suggested by Talbot and Woodward (2009), there are three sub-tasks suggested under the monitor operation: increase policy enforcement, build checking and reporting system on policy compliance, and establish non-compliance reporting.

These are the general consideration behavior of policy enforcement. The most common example in review trend and management sub-task is reviewing the policy (Doherty &Fulford, National computer board Mauritius, Woodward, and etc.). If the result of reviewing shows that the policy doesn’t fit the current security need, the development cycle should start from the very beginning, from building a security team, in order to develop a new policy to suit the current requirements.

7 METHODS IN DEVELOPMENT OF INFORMATION SECURITY POLICY

In this section, the research methods in the development of information security policy are listed. Table 4 shows the number of articles which have "research methods" provided, or at least give some suggestions in the development of information security policy. The research methods are separated into two categories: qualitative research methods and quantitative research methods.

Table 4: Methods for Development of Information Security Policy

Methods used for information security policy development		**Numbers**
Literature review		5
Qualitative	Interview	4
	Theory Deductive	2
	Case Study	3
Quantitative	Questionnaire Survey	7
Authors thought		49

7.1 Qualitative

Qualitative research is aiming to understand a certain phenomenon based on qualitative data. The purpose of qualitative research is to explore the meaning of people's experiences, cultures, or their understanding of a particular issue. The research questions of qualitative research are often started with "what" or "how". The analyzing of qualitative data is to create themes or theories.

7.1.1 Interviews

The qualitative interview is one of the data gathering methods in qualitative research. It is used in all kinds of qualitative researches includes positivist, interpretive or critical. Myers and Newman (2007) point out that the qualitative interview provides data with high-quality in case studies, action research, grounded theory, and in ethnographies. The key success factors for a quality interview is picking the right persons to interview and gathering the relevant data from the interviewees. However, it is difficult to achieve.

The forms of a qualitative interview are diverse, but three are most used: structured interview, unstructured or semi-structured interview, and group interview. A structured interview often contains a complete script for preparing beforehand. No space for change or improvisation in a structured interview. A structured interview is usually applied in surveys. An unstructured or semi-structured interview, however, contains an incomplete script. The researchers should have some preparation, in the meantime, there is room needed for improvisation. A group interview is just a structured or unstructured interview contains two or more people at once.

The qualitative interview is useful but embedded with potential problems, difficulties, and pitfalls. Based on the study of Web and his colleagues (1966) on the interviews, nine problems are summarized as typical examples of difficulties and problems in interviews. The nine problems are: artificiality of the interview, lack of trust, lack of time, level of entry, elite bias, Hawthorne effects, constructing knowledge, ambiguity of language, and the interviews can go wrong. (Myers and Newman, 2007) Take "lake of trust" as an example, the interviewer is a total stranger to the interviewee. Considering of security or privacy issues, the interviewees may refuse to provide some information which they consider as "sensitive". If the "sensitive" information is the potential important information for the research, this interview could consider as a failure.

There are four articles building their information policy theory based on interviews. Interview, as one of the research methods in a qualitative study, have the outstanding capability in building theories. Two target groups stand out in the literature reviews which support to formulate the methods in development of information security: information system security professionals and senior management groups. The interviews of those people are a useful support in the development of information security policy because they understand better in information security domain. They could provide professional knowledge and suggestions in information security management.

7.1.2 Theory Deductive

Theory deductive is a research strategy in scientific research. There are three steps to accomplish a theory deductive research: find a grounded theory, observation, build a new theory. It is a research strategy to build a specific theory from a general theory. The aim of the theory deductive is to conform or test a theory. The general theory usually guides the research process.

There are just two articles used theory deductive approaches to developing information security policy. Authors used IS design theory to develop the security policy. The similarity and commonality of design purpose in information system and information system security policy makes the IS design theory perfect suitable for the design of information system security policy.

7.1.3 Case Study

A case study research is an empirical investigation of a contemporary phenomenon, based on the study of Yin (1994). Case studies should be based on multiple resources of evidence. Case study research is one of the most commonly used qualitative research method in information systems research. (Darke, Shanks & Broadbent, 1998) The case study research is suitable for understanding the interplay between IT-related innovations and organizational situations. A case study is basically a combination of all data collecting technologies includes interview, observation, questionnaire, and document and context analysis. All qualitative and quantitative data collecting and data analyzing methods could be used in a case study research based on its research purpose. A case study research could reach several research goals: to describe the phenomenon, to develop a theory, and to test a theory.

There are three articles based on case study. There will be a real case such are the development of an information security policy for health care establishments. Also, there are simulated cases for testing the policy development method providing by the authors. The case study might not provide a generic method which could be used in most cases, however, it provides a specific point of view in concrete situation. The scope and applicability of information security policy in a healthcare center differ to the policy designed for an education institution. Case study method helps developing the proper information security policy for the particular requirements.

To build a theory from case study research, Eisenhardt (1989) provides eight steps. The suggested theory building phases are: getting started, selecting cases, crafting instruments and protocols, entering the field, analyzing data, shaping hypotheses, enfolding literature, reaching closure. These eight steps might not all concluded in the development of information security policy, however, these could be a guideline to start.

7.2 Quantitative

Qualitative research is aiming to examine the relationship between variables. The research questions of a quantitative research are started not only “what” and "how" but also includes "does" to study the relationship. Qualitative data often represents the statistics to crunch the numbers.

7.2.1 Questionnaire Survey

The questionnaire survey, invented by Sir Fransic Glaton, is a research tool to seize responses form respondents to study a common behavior based on a set of questions. The questionnaire survey consists structured or unstructured questions. A structured question provides respondents with a series of choice while an unstructured question needs respondents to answer with their own words. The questionnaire should be a series of questions designed to guide the respondents to understand the survey and provides the useful and high-quality data.

The most common used questionnaire survey is self-administered mail survey. The same questionnaire would be sent to groups of potential target respondents and willing respondents could finish the survey by themselves and return it to the research. Another type of a questionnaire survey is group-administered questionnaire. The questionnaire survey will be completed in a common place or a room by a sample of respondents. The purpose of this kind of survey is to limit the interactions between respondents. Recently, online or web survey is replacing the place of self-administrated mail survey. It is nearly the same as a self-administrated mail survey except the questionnaire form is electronic. It is more convenient for respondents to complete the survey as well as for researchers to analyze data. There are two major issues which obstruct researchers to reach the high-quality data. The first one is how to design a high-quality questionnaire which leads the respondents to give the needed data; the second on is how to determine the sample of respondents which are qualified to answer the questionnaire. In Chapter 9 Survey Research of the book Social Science Research, authors give some suggestions on question content and wording, question sequencing, and other golden rules for designing a questionnaire survey.

The questionnaire is the common used method to figure out the current security scale in the organization. It will test the end users' security behavior and the security strategy compliance within the organization. It could also be part of the risk assessment to analyze the need in protection of valid information stored in the system and transmitted via internet. The questionnaire is a nice start point in the development of information security policy.

7.3 Literature Reviews

The literature review is the method to study what have already existed in the domain of developing information security policy. Webster and Watson (2002) mentioned that "an effective review creates a form foundation for advancing knowledge". The purpose and value of literature review have already explained in the previews section since this thesis is based on literature review.

There are five articles are pure literature reviews of information security policy, however, there are more or less literature review studies included in every articles. It facilitates theory development, closes areas where a plethora of research exists and uncovers areas where research is needed. (Webster and Watson, 2002) Despite the previous scientific articles in information security management, there are some other documents which could be

7.3.1 Computer Security Document

SANS institution is a research and education organization established in 1989. It is, according to its website, the most trusted and by far the largest source for information security training and security certification in the world. Along with other information security company, SANS provides numerous security documents for information security policy development and implementation. The documents are formed by some literature reference and its security training programs.

7.3.2 International information security standards

According to Hone and Eloff (2002), international information security standards are the public standards in order to provide the generic information security above the world. It recognizes that information security policy is a major topic and it is covered early on the different standard documents. To name some of the information security standards as an example, there are BS7799, BSI, COBIT and etc. It is easy to pick the common elements and characteristics mentioned in the international security standards and use them as a start point in the development of information security policy.

7.3.3 Policy document in organizations

There are also four policy documents from organizations such as information security policy for London University. These policy documents are already applied in real life. They are a good example for studying the information security policy development. Policy documents which are already used in the organization give a realistic and reliable model for developing security policy in the same domain.

It could be seen from the table that most of the articles providing guidance for developing security policy are based on authors thought. At least none research methods are mentioned in the article about how they formulate the theory. It mainly caused by two reasons. Firstly, there are some organizational documents in the reference lists. The findings or decisions mentioned in organizational documents such as SANS security paper could not reach the cautious attitude as a scientific paper published in a professional journal such as MIS Quarterly. Secondly, information security policy development studies in scientific domain are still at the early stage. There is none systematical way to examine or test the proposed theory like IS development method. Due to the nature of information security policy and its diversity, it remains to be discussing which should be the effective method to develop information security policy with high quality and suit the requirements of the organization.

In the meantime, more than half of the papers (forty-nine out of eighty-three) are based on authors' thoughts. No obvious or direct research method is mentioned in those papers. The lacking of research methods are caused by two main reasons. On one hand, there are a certain proportion of company documents and existing policy documents in the analyzing reference. Those documents do not need to provide research methods to support their views. On the other hand, some authors of the scientific papers are security specialists who have the knowledge authority to give suggestions on information security policy development based on their previews experiences without providing any research methods.

8 DISCUSSION

This section answers the research questions defined in the previews sections. Also, some recommendations are given for the future research about the research questions and other relevant issues about information security policy development within organizations.

8.1 Functions of Information Security Policy

Based on the context analysis of descriptions of information security policy objectives and definitions, I summarized eight functions which should be achieved by information security policy. Information security policy within organizations should fulfill at least these eight functions. Information security policy is able to: represent the security strategy, plan the security requirements, define roles and responsibilities, define rules and protocols, state punishment, reduce risks, assist decision making, and provide a secured environment for business. However, information security policy exists in different forms. Some security policies are aiming to protect specific targets such as IT systems, emails, and password. For these security policies, they will have more detailed functions which are not included in this thesis. Also, functions of information security policy will alternate based on organizational requirements. These will be left to the future researchers to summarize.

8.2 Stakeholders of Information Security Policy

According to the study provided by Maynard, Ruighaver, and Ahmad (2011), there are nine kinds of stakeholders should be involved in the development of information security policy. The nine stakeholders are executive management, business unit representatives, user community, human resources, ICT specialists, external representatives, legal &regulatory, security specialists, and public relations. These nine stakeholders are summarized by literature reviews and tested by five security experts. Maynard, Ruighaver, and Ahmad (2011) point out that for medium to large organizations, all nine stakeholders should be involved; for smaller organizations, some of the stakeholder roles could be outsourced.

Despite the study provided by Maynard, Ruighaver, and Ahmad (2011), there are none another solid study on this domain. Although there might be several articles mentioned about stakeholders in sentences or paragraphs, it is missing in most of the studies. This is a huge gap in information security policy development study and should be fulfilled. For instance, there are no relevant materials or studies aiming to specify how and in which developing phases the stakeholders are involved. It is suggested by the authors to use the case studies method to determine what involvement of every stakeholder roles.

8.3 Information Security Policy Development Lifecycle

In order to formulate the information security policy development lifecycle, Table 3 is created to analyze the development phases provided in every article which provides development phases of information security policy. A lifecycle (Figure 3) is created by the generalization of the mentioned phases. There are five phases summarized from the analyzing which are: formulating a security team, assessment, plan, deliver, and operate. This lifecycle of information security policy is a generalization form from varies of lifecycles. However, this integrated information security policy development lifecycle is still remained to be tested in practice domain. This lifecycle could only be applied if it fits the organizational needs. Also, this development lifecycle is suitable for a general size organization. Depending on the size and business strategy, the development phase could be ignored or extended. Thus, more research and practical study should be done based on this development lifecycle to erase the limitations.

8.4 Methods in Development of Information Security Policy

According to the conceptual research, there are five methods to develop information security policy within organizations. The five methods mentioned in the literature review are: systematical reviews, interviews, questionnaire, theory deductive, and case study. However, a lot of articles provides information security policy development suggestions without any development methods. Forty-nine articles are just offering guidance based on authors' opinion.

These five methods are supported by at least one case. A few are supported by multiple cases. All five development methods prove their capability on the development of information security policy. However, most of them are not tested in practice domain. There are two major gaps missing in the methods of information security policy development. On one hand, these five methods should be tested after the development phase to detect the effort of the methods. On the other hand, the development methods should be categorized by the development phases. Since the methods are focusing on different targets, the different development methods should be categorized by is capability and output. This categorization will assist the security group to pick the right method to develop information security policy for their own organization.

8.5 Implications for Practice and Research

From the practical perspective, this review based study gives a clear view of how to develop information security policy within an organization. Firstly, it elaborates the functions of information security policy. This assists decision maker and employees within organizations to understand the importance of information security policy and what it could be achieved by development of information security policy. In the meantime, this study indicates all the stakeholders who should be involved in the development phase of information security policy. It depends on the organizational choice to select who should be involved in their policy development. Moreover, this reviewed study proposed a generalized information security policy development lifecycle. There are two practical purposes for organizations. On one hand, this lifecycle could determine what development phase the organizational security policy is current at; on the other hand, the lifecycle guides the following work of development in information security policy. The last but not the least, this study generalized five development methods for the organization to choose. Decision makers within organizations could choose one or multiple methods to develop the information security policy. All in all, the practical meaning of this reviewed study is a guidebook for the organization to develop their information security policy.

This study also has some contributions to research in information security policy. This thesis aims to have an overview of the current research in information security policy, and analyze the development phases of information security policy. For the research point of view, one essential contribution is that it summarized the functions of information security policy based on a large quantitative of views. It gives clear function descriptions about information security policy. Another essential contribution to the academic field is that it is one of the first vary researches to analyze the development phases provided from different papers. It has been concluded 29 kinds of development phases from different authors and integrated an information security policy development lifecycle. The study finding emphasized the essential position of information security policy in information security management and the representative of security strategy. It also detected the research gap which should be fulfilled but missing in current studies. For the practical point of view, the study provided five methods in the development of information security policy. It also integrated a development lifecycle for the security team to follow. The development lifecycle could lead the development steps by steps.

8.6 Future Research

The importance of information security policy is recognized by the executive management within organizations. However, the study and research on information security policy are just started. There are still many gaps need to be fulfilled. Information security policy development is a continued work, so is the study of information security policy.

Despite the researcher questions mentioned in this thesis, another research domain of information security policy is the integration of organizations' business strategy. As mentioned in the previews section, one of the information security functions is to represent the security strategy within the organizations. Since the priority of the organizational purpose is to run the business, the organizational security strategy is aiming to support the organizational business strategy. Thus, information security policy is one component to support the business contingency.

However, the research on this domain is nearly blank. Research questions like "What is the role of information security policy in the organizational business strategy?" or "How could information security policy support the business strategy?" are still remained to answer by professional researchers in the security management domain. Understanding the interaction between business strategy and the development of information security policy will assist creating an effective and high-quality security policy within organizations. On the other hand, studying of this interaction will help the organizations which already have an existing policy to modify and suit the business requirement.

Another research direction is to study the cultural difference in development of information security policy. Most of the studies on the development of information security policy are aiming to provide a generalized framework as a result for policy development. The organizational size and organizational culture are both considered as one dimension. Thus, the research results are more an overall-suggestion than a specific guideline. However, it is obvious that cultural difference and the organizational size while considering the information security policy development.

Tsohou, Karyda, and Kokolakis (2006) information systems risk management strategies could be formulated via cultural theory. Four cultural theories are assisting formulating the risk management strategies which are fatalism, hierarchy, individualism, and egalitarianism. These cultural theories should also affect the development of information security policy, especially the context of the policy. However, this is missing in the current study.

It is safe to announce that there are many researches should be accomplished in the future study. Information security management is a long-term study and it alternates based on organizational requirements. As the foundation of information security management, information security policy is also a long-term study with learning and development. Studies about information security policy should keep going on as long as information owns the value in business.

9 CONCLUSIONS

Information security management is an essential part of the organizational management in the age of information. Information security policy, as one of the foundation in information security management, has an unignorably state in organizational management. It is not only a management method in information security but also a representative of security strategy within an organization. There are series of studies on the topic of information security policy. In order to have an overview on current studies in information security policy, this thesis did a literature review on lists domains in information security policy: functions of information security policy; stakeholders in information security policy development; information security policy development lifecycle; and information security policy development lifecycles.

This thesis answered all the research questions based on 83 relevant references. It summarized the general functions of information security policy and the stakeholders involved in development phases. Basically, there are eight functions could be achieved by all kinds of information security policy. Meanwhile, nine stakeholders should be involved in the development phase of information security policy. It also integrated an information security policy development lifecycle and explains the meaning of each development phases. The information security policy lifecycle is formed by five development phases: formulate a security group, assessment, plan, deliver, and operate. In the meantime, it has been summarized about all the development methods mentioned in these articles. Five development methods are mentioned in the references. They are interviews, questionnaire, theory deduction, case study, and literature reviews. At last, research perspectives for the future are provided for the researchers in the same domain. The study finding indicates there are valuable studies in information security policy about the relevant domains. However, there are still research gaps to fulfill in the same domains.

9.1 Limitations

Like others, this thesis is not without limitations. One obvious limitation is the limited numbers of the references. The more valuable views this paper could provide based on the more reference I could access. However, as a master-degree student, I have less access right to the research papers especially the latest ones. It definitely affected the result of this thesis. In the meantime, some of the references are company documents or other papers from organizations. Thus, the views and suggestions provided in these documents are just based on author's opinions without any theories or data to support. The summarization of this thesis, due to this reason, might be affected by personal thoughts.

LIST OF REFERENCES

Abrams, M., & Bailey, D. (n.d.). *Abstraction and Refinement of Layered Security Policy.*

Albright, J. G. (2000). *The Basics of an IT Security Policy*. SANS Institudes.

Anderson, R. (1996). *A Security Policy Model for Clinical Information Systems*. In Proceedings of the IEEE Symposium on Security and Privacy, 30–43.

Antón, A. I., & Earp, J. B. (2000). *Strategies for developing policies and requirements for secure electronic commerce systems*. E-Commerce Security and Privacy, 2, 29–46.

Avolio, F. M., Consulting, a., Fallin, S., & Pinzon, D. S. (2007). *Producing Your Network Security Policy*. Watchguard. Com. July, (July), 1–13.

Banks, S. (1990). *Security Policy*. Computer & Security, 9, 605–610.

Baskerville, R., & Siponen, M. (2002). *An information security meta-policy for emergent organizations*. Logistics Information Management, 15(5/6), 337–346.

Bhattacherjee, A. (2012). *Social Science Research: principles, methods, and practices.* Textbooks collection (Vol. 9).

Bowden, J. S. (n.d.). *InfoSec Reading Room Security Policy : What it is and Why - The Basics*. Information Security.

Cardiff and Vale University Health Board. (2015). Information Technology Security Policy, 2003(23).

Chang, S. E., & Ho, C. B. (2006). *Organizational factors to the effectiveness of implementing information security management*. Industrial Management & Data Systems, 106(3), 345–361.

Clark, D. D., & Wilson, D. R. (1987). *A Comparison of Commercial and Military Computer Security Policies*. Nist Special Publication Sp.

Classification Security & Secretary, T. A. (2013). *Information security management policy*, (June 2010), 1–12.

Control Data. (1999). *White Paper: Why Securiy Policies Fail.*

Corpuz, M. (2011). *Enterprise information security policy assessment: an extended framework for metrics development utilising the goal-question-metric approach.* Proceedings of the 15th World Multi-Conference on Systemics, Cybernetics and Informatics.

Corpuz, M. (2011). *The enterprise information security policy as a strategic business policy within the corporate strategic plan*. Proceedings of the 15th World Multi-Conference, 275–279.

Corpuz, M. S. (n.d.). *Limitations of the Information Security Management System Assessment Approaches in the Context of Information Security Policy Assessment.*

Cosic, Z., & Boban, M. (2010). *Information security management - Defining approaches to information security policies in ISMS*. SIISY 2010 - 8th IEEE International Symposium on Intelligent Systems and Informatics, 83–85.

Danchev, B. D. (n.d.). *Building and Implementing a Successful Information Security Policy*. WindowsSecurit.com.

Darke, P., Shanks, G., & Broadbent, M. (1998). *Successfully completing case study research: Combining rigour, relevance and pragmatism*. Information Systems Journal, 8(4), 273–289.

Doherty, N. F., & Fulford, H. (2006). *Aligning the information security policy with the strategic information systems plan*. Computers & Security, 25(1), 55–63.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). *The information security policy unpacked: A critical study of the content of university policies*. International Journal of Information Management, 29(6), 449–457.

Eloff, J. H. P. (1988). *Computer Security Policy: Important Issues*. Computer & Security, 7, 559-562.

Enhancing Cyber Security in Mauritius. (2011). *Guideline on Information Security Policy*, (4).

Finance, S. (2011). *Information Security Policy, Procedues, Guidelines*. State of Oklahoma, (August), 1–5.

Galletta, D. F., & Hufnagel, E. M. (1992). *A Model of End-User Computing Policy - Context, Process, Content and Compliance*. Information & Management, 22(1), 1–18.

Gaunt, N. (1998). *Installing an appropriate IS security policy*. International Journal of Medical Informatics, 49(1), 131–134.

Gohuen, J. A. and Meseguer, J. (1982). *Security Policies and Security Models*.

Gritzalis, D. (1997). *A baseline security policy for distributed healthcare information systems*. Computers & Security, 16(8), 709–719.

Grobler, T., & Von Solms, S. (2004). *Assessing the Policy Dimension*. Policy, Vol. 64(1), 99–110.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). *Implementation and effectiveness of organizational information security measures*. Information Management & Computer Security, 16(4), 377–397.

Harlow, J. (2010). Security Policy- an individual view, 4(3), 87–113.

Harrison, W. L., & Dick, M. E. E. (1987). *An investigation of microcomputer policies in large organizations*. Information and Management, 12(5), 223–233.

Helwig, S. M. (2000). *Security Policy for Higher Educational Institudes*. SANS Institude.

Höne, K., & Eloff, J. H. . (2002). *What Makes an Effective Information Security Policy?* Network Security, 2002(6), 14–16.

Höne, K., & Eloff, J. H. P. (2002). *Information security policy – what do international information security standards say?* Computers & Security, 21(5), 402–409.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). *An integrated system theory of information security management*. Information Management & Computer Security, 11(5), 243–248.

Hostland, K. (2010). *Information Security Policy*. Uninet Led Working Group on Security, (October), 6–27.

Howard, P. D. (2002). *THE SECURITY POLICY LIFE CYCLE : FUNCTIONS AND RESPONSIBILITIES*.

Hu, J. (2009). *Idea to derive security policies from collaborative business processes*. Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC, 243–246.

Ilioudis, C., & Pangalos, G. (2000). *Development of an Internet Security Policy for health care establishments*. Med Inform Internet Med, 25(4), 265–73.

Institute of Education University of London. (2007). *Computer Security Policy*. IOE Information Security Policy: Effective: 1 July 2007

ISSAI. (1995). *Information System Security Review Methodology*, 91.

Jarmon, D. (2002). *A Preparation Guide to Information Security Policies*.SANS Institude.

Kadam, A. W. (2007). *Information Security Policy Development and Implementation*. Information Systems Security, 16(5), 246–256.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). *Information systems security policies: a contextual perspective*. Computers & Security, 24(3), 246–260.

Kee, C. K. (2001).*Security Policy Roadmap-Process for Creating Security Policies*. SANS Institude.

Klaic, A., & Hadjina, N. (2011). *Methods and Tools for the Development of Information Security Policy – A Comparative Literature Review*. Mipro, 1532–1537.

Klaiü, A. (2010). *Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies*, 1203–1208.

Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). *Information security policy: An organizational-level process model*. Computers & Security, 28(7), 493–508.

Lee, R. D. (2004). *Developing Effective Information Systems Security Policies*. SANS Institude.

Lichtenstein, S. (1997). *Developing Internet Security Policy for Organizations*. IEEE. 1060-3425/ 97

Lindly, J. P. (2001). *Technical Writing for IT Security Policies in Five Easy Steps*. SANS Institude.

Lindup, K. R. (1995). *A new model for information security policies*. Computers & Security, 14(8), 691–695.

Long, G. P. (2002). *Security Policies in a Global Ogranization*. SANS Institude.

Lopes, I. M. (2010). *Information Systems Security Policies : a Survey in Portuguese Public Administration*. IADIS International Conference Information Systems, 61–69.

Luker, M., & Petersen, R. (2003). *Policy Development for Information Seucirty*. Computer and Network Security in Higher Education Information Security. A Publication of EDUCAUSE.

Maynard, S. B., & Ruighaver, A. B. (2002). *Evaluating IS Security Policy Development. Security*, 183–189.

Maynard, S. B., Ruighaver, A. B., & Ahmad, A. (2011). *Stakeholders in Security Policy Developmen*t. 9th Australian Information Security Management Conference.

McConnell, K. D. (2011). *How to Develop Goof Security Policies and Tops on Assessment and Enforcement*, SANS Security Essentials, GSEC Practical Assignment, Version 1.3.

Myers, M. D., & Newman, M. (2007). *The qualitative interview in IS research: Examining the craft*. Information and Organization, 17(1), 2–26.

Oldehoeft, A. E. (1992). *Foundations of a Security Policy for Use of the . National Research and Educational Network*, (February), 1–64.

Olnes, J. (1994). *Development of security policies*. Computers & Security, 13(8), 628–636.

Palmer, M. E., Robinson, C., Patilla, J., & Moser, E. P. (2000). *META Security Group Information Security Policy Framework*. META Security Group.

Palmer, M. E., Robinson, G., Patilla, C. & Moser, E. P. (2001) *Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age*. Information Systems Security.

Pathari, V., & Sonar, R. (2012). *Identifying linkages between statements in information security policy, procedures and controls*. Information Management & Computer Security, 20(4).

Peltier, T. (2004). *Developing an Enterprisewide Policy Structure*. Information System Security, 31(8), 15–24.

Perkins, J. (2008). *Policy-Information Security Policy*. Proceedings of the 4th Annual Workshop on Cyber, (July), 1–3.

Pounder, C. (2002). *Security policy update*. Computers and Security, 21(7), 620–623.

Rees, J. Bandyopadhyay, S. & Spafford, E. H. (2015). *PFIRES: A Policy Framework for Information Security*.

Rogerson, K., & Milton, D. (2013). *A Policymaking Process "Tug-of-War": National Information Security Policies in Comparative Perspective*. Journal of Information Technology & Politics, 10(February), 462–476.

RSA Security Inc. (n.d.). *A Guide to Security Policy: A Primer for Developing an Effective Policy*.

SANS Institude (2007).*Information Security Policy-A Development Guide for Large and Small Companies*.

Schlarman, S. (2001). *The People, Policy, Technology (PPT) Model: Core Elements of the Security Process*. Information Systems Security, 10(5), 36.

Singh, A., Ramakrishnan, C. R., Ramakrishnan, I. V., Stoller, S. D., & Warren, D. S. (2007). *Security policy analysis using deductive spreadsheets*. Proceedings of the 2007 ACM Workshop on Formal Methods in Security Engineering - FMSE '07, 42–50.

Siponen, M. & Iivari, J. (2006). *Six Design Theories for IS Security*. Journal of the Association for Information System, 7(7), 445–472.

Siponen, M., & Willison, R. (2009). I*nformation security management standards: Problems and solutions*. Information & Management, 46(5), 267–270.

Smith, H. J. (1993). *PRIVACY POLICIES AND PRACTICES INSIDE THE ORGANIZATIONAL*. Business Computing, 36(12).

Solms, R. Von. (1999). *Information security management: why standards are important*. Information Management & Computer Security, 7(1), 50–58.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). *Information security policies in the UK healthcare sector: A critical evaluation*. Information Systems Journal, 22(1), 77–94.

Talbot, S., & Woodward, A. (2009). *Improving an organisations existing information technology policy to increase security*. Proceedings of the 7th Australian Information Security Management Conference, 120–128.

Tuyikeze, T., & Pottas, D. (2010). *An Information Security Policy Development Life Cycle.* South African Information Security Multi-Conference, (Saismc), 165–176.

Univeristy of Colleges Information Systems Association. (2015). I*nformation Security Edition 3.0.*

Unterkalmsteiner, M., Gorschek, T., Islam, a. K. M. M., Permadi, R. B., & Feldt, R. (2012). *Evaluation and Measurement of Software Process Improvement—A Systematic Literature Review*. IEEE Transactions on Software Engineering, 38(2), 398–424.

Von Solms, B., & Von Solms, R. (2004). *The 10 deadly sins of information security management*. Computers and Security, 23(5), 371–376.

Von Solms, R., Thomson, K. L., & Maninjwa, P. M. (2011). *Information security governance control through comprehensive policy architectures*. 2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference.

Ward, P., & Smith, C. L. (2002). *The Development of Access Control Policies for Information Technology Systems*. Computer & Security, Vol 21. No 4, pp356-371.

Watson, J. P. (2002). *Developing an Enterprise Information Security Policy*. 153–156.

Webster, J. and Watson, R. (2002). *ANALYZING THE PAST TO PREPARE FOR THE FUTURE: WRITING A LITERATURE REVIEW.* MIS Quaterly Vol. 26 No. 2, 42–49.

Wiant, T. L. (2005). *Information security policy's impact on reporting security incidents*. Computers & Security, 24(6), 448–459.

Wood, C. C. (1995). *Writing infosec policies*. Computers & Security, 14(8), 667–674.

Wood, C. C. (1996). *A policy for sending secret information over communications networks*. Information Management & Computer Security, 4(3), 18–19.

APPENDIX 1

Title	Authers	Year	Abstract
A baseline security policy for distribute healthcare information systems	Dimitris Gritzalis	1997	The paper offers an abstract approach for developing information security policy for healthcare information systems
A comparison of commercial and military computer security polices	David D. Clark-David R. Wilson	1987	A system integrity rules is formed based on the comparison.
A model of end-user computing policy: context, process, content and compliance	Dennis F. Galletta, Ellen M. Hufnagel	1992	A mail survey was formed to support the contingency theory of EUC policy compaliance.
A new model for information security policies	Kenneth R. Lindup	1995	Describe the existing types of security policy and deploy a new enterprise model which contains new treat and need security policy.
A policy for sending secret information over communications networks	Charles Cresson Wood	1996	Short discussion about policy for secured communication networks
A policymaking process" Tug-of-war": national information security policies in comparative perspective	Kenneth Rogerson, Daniel Milten	2013	The situation of the "tug of war" in the policies cause the incremental policy change an implementation
A preparation guide to information security policy	David Jarmon, SANS institute	2002	The processes before and within creating a security policy
A security policy model for clinical information systems	Ross J. Anderson		The paper discussed the relationship with current existing security policy models based on the case scenario of healthcare information security
Abstraction and refinement of layered security policy	Marshall Abrams and David Bailey		Chapter 5 in information security, gives layered view of policy which helps understand the rationale for security policy
Aligning the information security policy with the strategic information systems plan	Neil F. Doherty, Heather Fulford	2005	The paper develops the information security policy under the support of the strategic information systems plan.
An information security meta-policy for emergent organizations	Richard Baskerville and Mikko Siponen	2002	The paper explains the reason why meta-policy is needed for emergent organizations. A meta-policy is proposed for handling the policy formulation, implementation, en-

			forcement and validation.
An information security policy development life cycle	T. Tuyikeze and D. Pottas	2010	The paper illustrates the current methods in security policy development and formulates a information security development life cycle
An investigation of microcomputer policies in large organizations	William L. Harrison, Mary Ellen E. Dick	1987	This research measures the content to which microcomputer policies are in place and classifies the nature of the policy statement
Assessment the policy dimensions	T Grobler, Prof SH von Solms		The paper offers a policy framework and explain the relationship between policy dimensions.
Build and implementing a successful information security policy	Dancho Danchev	2003	The paper outlines the strategies and managing process in implementation a successful security policy
Computer security policy	Institution of Education University of London	2007	Detailed policy applied in institution of education university of London
Computer security policy: important issues	Dr Jan H.P. Eloff	1988	This paper addresses importance issues in compiling a computer security policy
Develop Internet security policy for organizations	Sharman Lichtenstein	1997	It provides a general framework for developing an organization's Internet security policy
Developing an enterprise information security policy	Jinx P. Walton	2002	It is a three-year strategic plan on information technology in the university of Pittsburgh. It is a step by step security management plan to develop information security policy
Developing an enterprise wide policy structure	Thomas R. Peltier	2004	The paper provides at least 12 tier 1 policies that every organizations must address
Developing effective information systems security policies	R. Daniel Lee SANS Security Essential	2001	It offers a high-level overview for developing effective information security policies based on a top-down approach
Development of an internet security policy for health care establishments	Christos A. Ilioudis, George I Pangalos	2000	This paper describes an appropriate internet security policy for heal care establishments and provides technical measures that are needed for implementation
Development of security policies	Jon Olnes	1994	This paper help developing a security policy based on a figure method and its countermeasures.
Enterprise information security Policy Assessment- an extended framework for metrics	Maria Soto Corpuz		The paper explain the goal-question-metric approach as security assessment approach in order to develop information security poli-

development utilizing the goal-question metric approach			cies
Evaluating IS security policy development	S.B. Maynard & A.B. Ruighaver		An initial approach is provided for evaluating the quality of the resulting security policy.
Foundations of a security policy for use of the national research and educational network	Arthur E. Oldehoeft	1992	The document contains the foundations for a national networks security policy and proposed security policy for use of the NREN
From policy to culture	Rossouw von Solm, Basie von Solms	2004	This paper addresses the process of integrating policies, education and culture
Guideline on information security policy	National computer board	2011	The document give detailed guidelines on information security policy includes purpose, structure, development process and etc.
How to development good security polices and tips on assessment and enforcement	Kerry D. MoConnell; SANS Security Essential	2000-2002	Approaches to develop effective security policy for organizations
Idea to derive security policies from collaborative business process	Ji Hu	2009	This paper introduces the current research for developing information security policy from formal business process models
Identifying linkages between statements in information security policy, procedures and controls	Vinod Pathari and Rajendra Sonar	2012	The paper proposes an approach to analyze the security statements and the linkage between them.
Implementation and effectiveness of organizational information security measures	Janne Merete Hagen, Eirik Albrechtsen, Trondheim Norway and Jan Hovden	2008	This paper is to study the implementation of organizational information measures and evaluate the effective of these measures.
Improving an organizational existing information technology policy to increase security	Shane Talbot, Andrew Woodward	2009	The paer give guidelines for improving policy development and approval process.
Information Security Edition 3.0	UCISA	2005 first edition	A book about information security
Information security governance control through comprehensive policy architectures	Rossouw Von Solms, Kerry-Lynn Thomson, Prosecutor Mvikeli Maninjwa		The paper has studied information security governance via the information security policy architecture
Information security management policy	Professor Geoff Whitty	2010	This document provides a information security policy for university of London

Information security management-defining approaches to information security policies in ISMS	Zoran Cosic, Marija Boban	2010	This paper gives an overview of defining security policies in ISMS
Information security maturity model	Dr Malik Saleh	2011	The paper proposed an information security maturity model to evaluate the ability of organizations to meet the objectives of security
Information security policies in the UK healthcare sector: a critical evaluation	Bernd Carsten Stahl, Neil F. Doherty & Mark Shaw	2012	This paper tries to analysis information security policy by viewing them through a critical theoretical lens in a case study of UK healthcare service
Information security policy best practice document	Kenneth Høstland, Per Arne Enstad, Øyvind Eilertsen, Gunnar Bøe	2010	The document contains a template of an information security policy
Information security policy development and implementation	Avinash W. Kadam	2007	This paper formulates an development approach for information security policy. It also contains the business impact and other implementing elements of information security policies
Information security policy development and implementation	Avinash W. Kadam	2007	The paper tries to formulate an approach to the information security policy development that makes policy document suitable for the application in business
Information security policy development and implementation: a content analysis approach	T. Tuyikeze and S. Flowerday	2014	A literature analysis about the challenges and approaches in development of information security managements
Information security policy framework: best practices for security policy in the E-commerce age	Malcolm E. Palmer, Craig Robinson, Jody C. Patilla and Edward P. Moser	2001	The META SeS information security policy framework
Information security policy, procedures, guidelines	State of Oklahoma	2015	The document presents the minimum information security policy, procedures, guidelines and best practices for protections of information assets
Information security policy: an organizational-level process model	Kenneth J. Knapp, R. Franklin Morris, Jr. Thomas E. Marshall,	2009	This paper formulates a model to illustrate a general yet comprehensive policy process based on depicting a larger organizational context

	Terry Anthony Byrd		
Information security policy's impact on reporting security incidents	Terry L. Wiant	2005	This article study the effectiveness information security policy in reporting of computer incidents
Information security policy-a development guide for large and small companies	Sorcha Canavan and Sorcha Diver SANS institute	2007	This document gives guidelines on elements in information security policies includes the requirements, the users, types, topics and etc.
Information security policy-what do international information security standards say?	Karin Hone and J.H.P. Eloff	2002	This paper reviews the international information security standards as a start point to develop information security policy
Information system security review methodology	ISSAI 5310	1995	This book describe what is information security, then methods and approaches to develop information system security
Information systems security policies: a contextual perspective	Maria Karyda, Evangelos Kiountouzis, Spyros Kokolakis	2005	This paper proposed a contextual framework of information security policy in four dimensions which affect their success adoption
Information systems security policies: a survey in Portuguese public administration	Isabel Marja Lopes, Filipe de Sa-Soares	2010	A development information security policy guideline for public administration based on a survey in Portuguese
Information technology security: key to success	Judith Borreson Caruso	2003	A survey research about the policy development in institutions.
Installing an appropriate information security policy	Nick Gaunt	1998	This paper shows the development and implementation of an information and security policy in the health care environment
Limitations of the information security management system assessment approaches in the context of information security policy assessment	Maria Soto Corpuz		The paper analysis the current situation of security policy assessment and how to evaluate assessment approaches in the context of information security policy assessment
META security group information security policy framework	Malcolm E. Palmer, Craig Robinson, Jody Patilla, Edward P. Moser	2000	This document offers a meta security group information security policy framework
Methods and tools for the development of information security policy- a comparative literature review	Aleksandar Klaic, Nikola Hadjina		This paper determines the actual states and trends in the domain of methods and tools in information security policy
Overview of the state and	Aleksandar	2010	This paper gives an overview of the

trends in the cotemporary information security policy and information security management methodologies	Klaic		domain of information security policy and IS management methodologies
PFIRES: a policy framework for information security	Jackie Rees, Subhajyoti Bandyopadhyay and Eugene H. Spafford		Using PFIRES life cycle model for developing information security policy
Policy Development for Information security-Computer and Network Security in Higher Education	Mark Bruhn and Rodney Peterson	2003	A general information security policy description and analysis
Policy: information security policy	Jethro Perkins	2015	It is a policy document released by London School of Economics and Political science
Privacy policies and practices: inside the organizational maze	H. Jeff Smith	1993	It is a survey study for analyzing the private policies and practices
Producing your network security policy	Frederick M. Avolio, Steve Fallin	2007	The process to creating a network security policy
Security policies and security models	J. A. Goguen and J. Meseguer	1982	The paper described an approach based on modelling the information processing system, defining security policy and verifying that a given system satisfies a given policy
Security policies in a global organizations	Gerald P. Long SANS institute	2002	A guideline to create information security policy for a global organization
Security Policy	Simon Banks	1990	General information about security policy in every domain.
Security policy analysis using deductive spreadsheets	Anu Singh, C.R. Ramakrishnan, I.V. Ramakrishnan, Scott D. Stoller, David S. Warren	2007	This paper proposed a deductive spreadsheets for security policy analysis
Security policy for higher educational institutions	Steven M. Helwig, SANS institude	2000-2005	A guideline for creating security policy for higher educational institutes
Security Policy Roadmap-Process for creating security polices	Chaiw Kok Kee SANS institute	2001	A step by step guideline for creating information security policy

Security policy update	Chris Pounder	2002	This paper reviews the recent public policies which will impact on an organizational approach towards the security of its data
Security policy: an individual view	John Harlow	2001	This paper describe the necessary of a information security and how individuals could be drawn up and implemented
Security policy: what it is and why	Joel S. Bowden, SANS institute	2003	A general description about information security policy and its capability
Six design theories for IS security policies and guidelines	Mikko Siponen, Juhanni Iivari	2006	The paper suggests six design theories and outline their application principles in guiding the application of IS security policies
Stakeholders in security policy development	S B. Maynard, A B. Ruighaver, A. Ahmad	2001	The paper identified stakeholders and their roles in information security policy development.
Strategies for developing policies and requirements for secure electronic commerce systems	Annie I. Anton, Julia B. Earp	2000	The paper provides specification strategies for security policy and requirements
Technical writing for IT security policies in five easy steps	J. Patrick Lindley, SANS institute	2001	Five steps for writing IT security polices
The basics of an IT security policy	Jack G. Albright, SANS institute	2002	The components of a security policy
The development of access control policies for information security technology systems	Peter Ward and Clifton L Smith	2002	The paper proposed a high level approach to implementing security policies of information assessment.
The enterprise information security policy as a strategic business policy within the corporate strategic plan	Maria Soto corpus		The paper proposed alignment approach for security policy as a strategic business policy and integrative approach for developing enterprise information security policy
The information security policy unpacked: a critical study of the content of university policies	Neil Francis Doherty, Leonidas Anastasakis, heather Fulford	2009	A critical study of university policies' content and the result concludes that the wide diversity policies in use is unlikely to foster a coherent approach to security management.
The people, policy, technology model: core elements of the security process	Steven Schlarman CISSP	2001	How to understand the PPT model and their relationships
The security policy life cycle: functions and re-	Patrick D. Howard,	2002	The paper proposed a policy function responsibility matrics

sponsibilities	CISSP		
What makes an effective information security policy	Karin Hone and J.H.P Eloff		The paper identifies what is an effective information security policy and how to achieve it.
Why security policies fail	Control Data	1999	The nature weakness of security policy and the security lifecycle
Writing infsec policies	Charles Cresson Wood, CISA, CISSP	1995	The paper offers guidelines how to write infosec policy after explaining the importance of policies