Association for Information Systems
AIS Electronic Library (AISeL)

All Sprouts Content

Sprouts

11-25-2011

Designing Information Systems Security Policy Methods: A Meta-Theoretical Approach

Asheesh Nigam
The University of Oulu, asheesh.nigam@oulu.fi

Mikko Siponen
The University of Oulu, msiponen@tols16.oulu.fi

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

Designing Information Systems Security Policy Methods: A Meta-Theoretical Approach

Asheesh Nigam
The University of Oulu, Finland

Mikko Siponen
The University of Oulu, Finland

Abstract
Information systems security policy (ISP) is the critical foundation of information systems security. Despite the criticality of the ISP, information systems security scholars have expressed concerns about the lack of theory and limited methodological support for the development of ISP. Existing literature on ISP Development (ISPD) is scattered and lack meta-theoretical approach toward designing ISPD Methods (ISPDM). This paper aims to fill the gap by consolidating extant ISPD approaches and put forth a systematic way by adopting a meta-theoretic approach in defining essential principles for designing ISPD method. After presenting the principles we demonstrate that none of the existing methods are based on all the essential principles.

Keywords: Information systems security policy, Information systems security policy methods, Meta-theory, Essential principles.

Permanent URL: http://sprouts.aisnet.org/11-150

Reference: Nigam, A., Siponen, M. (2011). "Designing Information Systems Security Policy Methods: A Meta-Theoretical Approach," Proceedings > Proceedings of JAIS Theory Development Workshop . *Sprouts: Working Papers on Information Systems*, 11(150). http://sprouts.aisnet.org/11-150

Designing Information Systems Security Policy Methods: A Meta-Theoretical Approach

Abstract

Information systems security policy (ISP) is the critical foundation of information systems security. Despite the criticality of the ISP, information systems security scholars have expressed concerns about the lack of theory and limited methodological support, especially which focuses on social and political issues, for the development of ISP. Existing literature on ISP Development (ISPD) is scattered and lack meta-theoretical approach toward designing ISPD Methods (ISPDM). This paper aims to fill the gap by consolidating extant ISPD approaches and put forth a systematic way by adopting a meta-theoretic approach in defining essential principles for designing ISPD method. After presenting the principles we demonstrate that none of the existing methods are based on all the essential principles.

Key words: Information systems security policy, Information systems security policy methods, Meta-theory, Essential principles**.**

1. Introduction

Scholars and practitioners widely agree that Information systems security policy (ISP) is the critical foundation of information systems security (David, 2002; Marcinkowski and Stanton, 2003; Corby 2007; Kadam, 2007). As a result, ISP is a standard issue of any books on information security management, and ISP is required by key information management standards. Despite the indisputable importance of ISP, information systems security scholars have criticized that the lack of theory and limited methodological support for the development of ISP (Olnes, 1994). Such situation is common for young disciplines or research topics, and scholars have cried out for more theory-development in such disciplines. A glance to history of philosophy of science suggests the importance of meta-theories and respective thinking. There are numerous examples in different fields of science as to how meta-theories, which are theories on theories or methods, had a fundamental influence on theories or methods, and in that way practice, in difference disciplines (Laudan 1990). Examples include meta-mathematics in terms of Hilbert, Friege, Russell and Richard (Good 1966), or meta-ethics in terms of Hare (1981) or Kant. Laudan (1990) expresses his concerns about the disconnections of exiting theories in terms of social and political issues. Drawing analogy to the ISP, while the importance of ISP has been recognized, there are limited meta-theoretical discussion on typical meta-theoretical issues, as to what are the meanings of the key concepts, what is the nature of ISP in terms of social and political influences, and their methods, and how ISP, ISP methods or ISP theories are validated (cf., Garner & Rosen 1967). Such discussion is important because a meta-theoretical approach can provide how scholars and practitioners can develop an ISPD method which addresses systematically a class of concerning issues, and can evaluate and select an appropriate ISPD method according to their needs. To address these issues, we argue that ISPD approach should be based on essential principles grounded on fundamental characteristics of ISPD process that are derived from meta-theoretical approach.

As a first step in remedying such situation in the literature we advance a meta-theory for ISP methods in this paper. The theory is based on five essential principles developed on fundamental characteristics of ISPD process. These characteristics are derived by applying structurational model in understanding the nature of interaction between ISP and organizations per se. These five principles preliminary based on addressing the security needs of organization, by preparing organizations how to address the need by involving employees and top management, and finally an easy and understandable security policy. After presenting essential principles, we find that none of the existing ISP methods are based on these essential principles.

The results of the study will serve the expectations of academics and practitioners alike in the field of ISP. For academics it will consolidate the existing research in the field of ISPD approaches. Further, it will offer a meta-theoretical approach in identifying and generalizing the fundamental characteristics of ISPD and how it takes into consideration the extant literature on the issue. Our study suggests essential principles based on meta-theoretical approach for designing ISPD tools / methods will be a valuable contribution for the practitioners.

Rest of the study is organized as follows. Next is literature review section. This followed by advancing a meta-theory for designing ISPD method. Then we elaborate essential principles for security policy methods and then demonstrate that none of the existing ISPD methods are based on all the essential principles. We discuss implications of this research for academics and practitioners, followed by a conclusion.

2. Extant ISPD approaches

ISPD methods offer a systematic approach for developing and implementing balanced and efficient security policy (Olnes, 1994). In contrary to the cumulative tradition of knowledge development, existing literature on ISPD approaches and methods are scattered and reflect lack of cumulative tradition. In order to follow the cumulative research tradition this study aims to analyze the extant ISPD methods and approaches from the viewpoint of (i) research objectives, and (ii) the organizational role of IS security, (iii) and robust founding of the approaches.

Analysis of the extant methods in the light of the research objectives is useful to highlight the possible goals of the researchers. Following Chua (1986) and Habermas (1984, 1987), potential research objectives include: a) means-end oriented/technical; b) interpretive; or b) critical/emancipatory objectives. It is important to understand which ISPD methods favor which types of organizational roles (cf., Iivari & Kerola 1983, Kant 1993, Iivari & Hirschheim 1996)? Possible organizational roles of information systems security includes: a) technical; b) socio-technical; or c) social. The viewpoint of robust founding addresses the concern of generalizability and utility of the ISP methods. The idea hails from the idea of philosophy of science. This approach also addresses academic concern about the rigor, by applying theory in developing ISP method. In fact, the whole idea of scientific research rests on theories: “The central role of theory in the scientific enterprise can hardly be challenged.” (Liska *et al.* 1989, p. 2). There are assertions for the practical utility of theories. If security policy approach lacks underlying theory, it would not be able to explain why certain approach works in any given condition and why certain approach does not work in the given conditions. This concern of utility also belongs to the philosophy of science concept, where the empirical evidence is often considered as the essential constituent of science. Such a need for testing theories empirically is highlighted by different philosophers of science. In the area of social sciences, Cao (2004) stresses that the cornerstone of science is the rigorous use of empirical research methods, including making the reporting of the research results and research process visible. Akers and Sellers (2004 p. 5) share this view: the ultimate test of a theory is it practical utility. Empirical evidence is important for practitioners to ensure that developed methods work in real world (Abrahamsson *et al*. 2003).

We find forty two extant ISPD approaches on some kind of prescriptions, guidelines, methods, processes, essential components, standards, frameworks or how to develop security policies. Out of the forty two approaches only three approaches have the research objective being interpretive, two means end oriented and and remaining thirty seven are conceptual analytical work. Methods / approaches that follow interpretive objective include Karyda *et al.* (2003), and Karyda *et al.* (2005) and Ferreira *et al.* (2010). Karyda *et al.* (2003), and Karyda *et al.* (2005) apply contextual theory in their work and also conducted empirical study to demonstrate the utility of their proposed framework. Karyda *et al.* (2005) find that their approach offer critical insights into the problems of ISP effectiveness and put forwarded to explore social oriented theories from the field of organization theories for focusing on broader range of issues of ISPD. Ferreira *et al.* (2010) applied grounded theory in their paper and suggest focusing on users' involvement approach during the entire process of security policy development and implementation. The two approaches that have means end objective have technical as organizational role. However, among the conceptual analytical approaches have social as organizational role of ISPD methods.

Out of forty two methods, there are only five methods that have robust founding but only two papers meet both the criteria of robust founding. Among these methods, method by Brewer and Nash (1989) is based on mathematical theory. Karyda *et al.* (2003) and Karyda *et al.* (2005)

applied contextual theory in their work and also conducted empirical study to demonstrate the utility of their proposed framework. Ferreira *et al.* (2010) applied grounded theory in their paper. Coles-Kemp and Theoharidou (2010) suggest security management process design based on the theories derived from the crime theories. The theories mainly applied are Social Bond Theory, Social Learning Theory and Theory of Planned Behavior for social aspects, while applied General Deterrence Theory only for differentiating compliance and non compliance aspects. Due to the limitations of these theories, their paper lack business aspects and hence their suggested process does not meet all the principles.

Generally speaking, the extant methods of ISPD hardly refer to the related work done by fellow scholars, not to mention the fact that their authors set their research problems in the context of the existing research on ISPD methods. However, science should be cumulative: it should build on the existing research (Laudan 1990). The lack of such a cumulative research tradition means that authors are inventing the wheel again and possibly repeating the same mistakes. This non-cumulative research practice also hinders the development of the field in general (cf., Klein & Hirschheim, 2003). Finally, this research practice confuses scholars and practitioners, who have serious difficulties in separating the numerous works on ISPD methods from each other (as the authors neglect to explain this, while they also use different terminology). Therefore, we argue that there is a need for approach that can consolidate existing research in this field and thus focuses on cumulative research tradition. However, the approach should be founded on theory based ISPD method to have a broader generalizability and thus larger applicability. We first understand the nature of ISPD process, and then by proposing meta-theoretical approach we systematically analyze the fundamental characteristics of ISPD process and interlace concerning issues through putting forth essential principles of designing ISPD methods.

3. Toward a New Meta Theory for Designing ISPD Methods

Information systems security policy development methodology (ISPDM) is interpreted as "an organized collection of concepts, methods, beliefs, values and normative principles supported by material resources" (Hirschheim et al., 1995). The purpose of the ISPDM is to help the organization effectively change the risk level of information systems security. Methodologies are termed as normative as they prescribe how to reduce the risks of information systems security. The definition of methodology focuses on organized collection due to the reason that methodologies cannot be randomly selected. Therefore we argue to have a meta-theoretical approach which can systematically explain the concepts, belief, values and methods involved in ISPD method design. By this approach we systematically analyze essential principles that are based on fundamental characteristics of ISPD method, which help in developing and implementing security policies that meet the purpose.

This paper primarily focuses on ISPD approaches and its fundamental characteristics, and does not intend to suggesting or recommending best security policies per se because of the two reasons. First reason, security policy differs from one organization to another due to differing security needs and requirements of these organizations due to their internal and external environments (Madnick 1978, Whitman et al 2001). Second reason, we argue that good content of a policy itself does not attribute to the desired outcome from security policy. Rather, the desired outcome from security policy stems on several interdependent factors such as organization preparedness, role of policy developers, involvement of top management, resource deployment, and motivation of users.

To uncover the fundamental characteristics of ISPD method we need understanding of the nature of ISP development process and its influence. ISPD process, an artifact for managerial intervention (Gregor and Jones, 2007) aimsto change the state of unsecured to secured information systems assets. ISPD methods, the artifact for brining change to securing information systems assets, comprise policy development approaches, methods, techniques and tools (Walls *et al.,* 1992). Therefore ISPD method being an artifact entails a change process taken with respect to information systems security. In terms of Hirschheim *et al.*, (1995), the role of artifact can be defined as to increase the state of security of information systems assets that is influenced by a set of environments, internal and external, implemented through a change process managed by a task force, who is given the objective to increase security of information systems assets. Hirschheim *et al.*, (1995) further stress that thus the role of artifact is mainly shaped by four components information systems security, change process, environments and taskforce, that suspend together in a web of social, cultural and technical phenomena. This implies that these components are interlinked and achieve a better outcome when work together. , which are mutually exclusive and collectively exhaustive.

Therefore, a theoretical framework which supports us in understanding the fundamental characteristics of ISPD process as mentioned above as an organizational change process and elaborates how these characteristics influence practices of ISP would be suitable for analysis. To achieve this, structurational model developed by Orlikowski & Robey (1991) based on the Gidden's theory of structuration is an ideal theoretical framework. The model is an ideal candidate framework for analyzing the ISPD process because of the following reasons: 1) it blends security policy development and usage together into one entity for analysis, Markus (1983) explains the criticality of linking development and usage in understanding the criticality of such issues. 2) The structuration approach not only focuses on policy influences users, but also how users influence policy. 3) The approach has been applied successfully in studying IS artifact induced organizational changes; 4) the approach in structuration theory fulfills the paucity of theory highlighted by Markus and Robey (1988). 5) It is a meta-theory that integrates multiple level of analysis (Orlikowoski and Robey, 1991) and thus can offer richer and deeper insights into the components of ISPD process.

Gidden's theory of structuration has been adopted by a number of organizational researchers in order to understand the organizational change process. Among others, Orlikowski & Robey (1991) found structuration theory useful in explicating the features of organizational change entailed by information technology. In their work Orlikowski & Robey developed a theoretical framework by focusing on information technology, and how information technology is created, used and become institutionalized within organization. Applying the same analogy, we adapt the same framework by focusing on ISP, and thus explicating how ISP is developed, implemented, adopted and become institutionalized within organization.

A structurational model of information security policy

Figure 1 depicts a generic structurational model of information systems security policy adapted from Orlikowski & Robey (1991). The model explicates four key influences that operate continuously and simultaneously in the interaction of between security policy and organizations: i) Arrow a – information security policy is the outcome of human action, being developed and used by humans; ii) Arrow b – ISP is the means of other human action, serving to facilitate the protection of information systems security; iii) Arrow c – ISP is developed, implemented and adopted within specific social context; and iv) Arrow d – interaction with ISP influences the social context within which it is developed, implemented and adopted. These four dimensions of ISSP and of the organization operate simultaneously (Orlikowski & Robey, 1991).

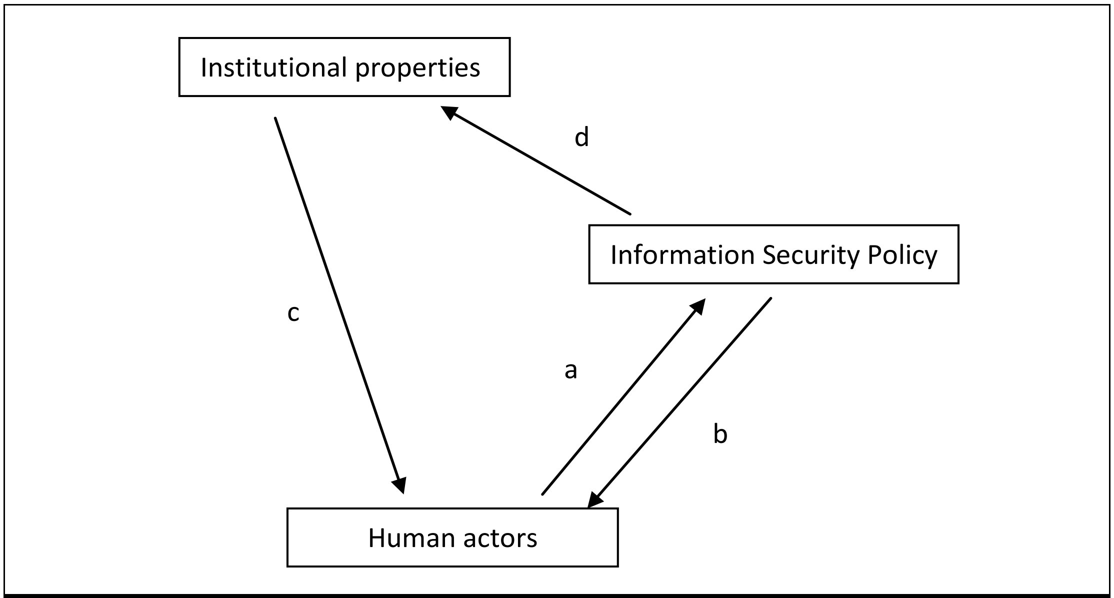

Figure 1 : Structurational model of Information systems security policy

The above model is based on the relationships between ISP and organizations, which is seen as two central themes in formulation and implementation of security policy: the process of ISSPD and the social consequences of security policy implementation. According to Gidden's view these two themes can be analyzed in terms of human actions /interactions that are linked through modalities (interpretive schemes, resources and norms) with institutional / social structure. This linkage between the realm of social structure and the realm of human action is referred to as the process of structuration (Giddens 1979). Further, Giddens (1984) explains the vitality of how modalities work within each of the institutional / social and human actions realms of organizations.

The realm of social structure and the realm of action in the ISSPD process: The team responsible for formulating security policy is influenced by their knowledge, resources available to the team, objectives of the top management and organizational form and culture (Orlikowski and Robey, 1991). ISSPD methodology assumes a critical role in facilitating and constraining these tasks of the team. The methodology of ISSPD would contribute in analyzing and interpreting the risk associated to the information systems assets, reshaping the power structure in terms of ownership and managing the security policy, and in developing policy and institutionalizing practices about policy development and implementation. The team responsible for security policy formulation and implementation takes action based on the risk analysis of external and internal environments, legal provisions for protecting information systems assets, rearrangement of roles and responsibilities in organizational structure for formulating and implementing security policy, and available tools for training employees and communicating with employees. Thus the ISSPD process, by placing realm of social structure and realm of action together, primarily consists of:

1) Tool for analyzing risks, from external environment and internal environment to information systems assets, according to objective of the top management.

2) Facilitates organizing the structure as required for formulating and implementing security policy.

3) Focuses on institutionalizing adherence to security policy by educating and communicating with employees.

The realm of social structure and the realm of action, and the social consequences of security policy implementation: The structural perspective emphasizes on how action of users are shaped by implementation of security policy. The modalities as embedded in a security policy mediate the behavior of users in adhering to security policy. Security policy an artifact of managerial intervention shapes the actions of users by facilitating certain objectives of the management and constraining others. Employees would judge the appropriateness of the security policy before adhering to (Orlikowski and Robey, 1991). In this situation it is recommended to engage employees, for whom this security policy is meant for, in understanding and elaborating the appropriateness of the policy. In interpreting the appropriateness of the security policy, resources and norms within the organization significantly influence employees. By referring to Kling and Iacono, Orlikowski and Robey (1991) explain that education, training and involvement of top management are important in establishing the pattern of change. Thus the social consequences, by placing realm of social structure and realm of action together, primarily have following influence:

1) Employees attempt to understand the security policy and adhere to it. They just follow the part of policy which they understand and gradually this pattern becomes institutionalized.

2) Employees evaluate the appropriateness of security policy before adhering to it; therefore involvement of employees is essential for appropriate security policy formulation.

3) Employees find provisions for education and communication, commitment of resources and involvement of management as source of motivation in adhering to security policy.

Characteristics of ISSPD method by relating ISSPD process and social consequences of implementing ISSP:

1. ISSPD process facilitates as tool for analyzing the internal and external environment of the organization. This tool serves the purpose of the objective of top management and in sustaining the business by increasing the security of information systems asset. Since the internal and external environment, objective of top management, and the purpose of organization differs from one organization to another, therefore security needs differ from one organization to another. Thus ISSPD process should facilitate formulating security policy founded on the need of the organization.

2. ISSPD process focuses on preparing organizations for formulating and implementing security policy. In terms of reorganizing there is a need for a team which would manage all the tasks. Since security policy serves the objective of top management and employees are motivated by top management involvement, therefore the team should have a representation from top management. The theme of social consequences has thrust on involvement of employees; therefore team should have representatives of all employees.

3. Institutionalizing adherence to security policy is suggested to achieve by educating and communicating with employees, therefore it is important to include all the employees in this process. In the process of institutionalizing, employees evaluate appropriateness of security policy therefore participation of employees is highly recommended. Thus employees, who are users of the security policy, should be involved in formulating and implementing security policy.

4. The entire process of ISSPD and adherence to security policy by employees entail various provisions such as analysis of risks, formulating security policy, educating and communicating with employees that consume resources. Allocation of appropriate resources for these activities is not possible without the commitment of top management to the appropriate security policy. Also, employees who institutionalize adherence to security policy see involvement of top management in the entire process as source of motivation.

5. The pattern of adhere to security policy gradually institutionalized within the organization. The pattern of adherence to security policy largely depends upon the simple and understandable language of security policy. If employees do not understand or wrongly understand the policy they would institutionalize the adherence as what and how they understand the policy.

Characteristics reflecting the principles of ISSPD method:

Table 1: Fundamental characteristics reflecting essential principles

Characteristics of ISSPD method	**Principles in designing ISSPD method**
Analyzing the internal and external environment, according to the objective of top management and in sustaining the business	Syncing with the need of organization
Preparing organization in terms of restructuring powers, roles, responsibilities	Organizational adaptability
Educating and communicating with employees, involving participation for appropriate security policy	Users’ involvement
Various activities involve immense resources in terms of money and time of top management apart from others	Top management commitment
Simple, practical and easy to understand policy which facilities proper adherence to full security policy	Cogent policy

4. Explicating the Principles of ISSPD methods

Principle 1. Syncing with organizational need

The principle of unique business need addresses the concerns that information systems security depending upon businesses are unique in nature, therefore ISPD process should focus on aligning policy with the unique business need. Marcinkowski and Stanton (2003) find that “security policies are unique in nature due to business objectives, legal requirements, organizational design, organizational culture, prevailing ethics and morals, extent of education of users, and technology deployed”. These factors influence threats and risks differently; therefore specific security requirements vary from organization to organization (Madnick, 1978). The same concerns Bensaou and Earl (1998) express that business practices are heavily influenced by national culture, industry traditions and company level characteristics, therefore copying benchmarking and best practices could be devastating by not incorporating the unique business needs. The concern can be understood as organizations have unique need in terms of protecting their information systems. Therefore neither single security solution nor a single security policy can fit all organizations (Whitman et al., 2001). Henceforth, the principle of syncing with organizational needs suggests that ISPD process involves developing and implementing policies that are internally consistent with strategic logic, aligned with business processes, and consequently match with organization’s business strategy (Marcinkowski and Stanton, 2003; Hayes 2006).

Resource-based view, advocates that in order to pursue purpose of the organizations, critical strategic assets must be protected. Barney (1991) refers to information and knowledge as critical firm resources due to the view that information systems is a rare, valuable, inimitable and immobile critical asset supports vision and mission of the organization. Resource-based theory also explains that a firm may develop any form of resources for sustaining its purpose (Selznick, 1957; Penrose, 1959; Wernerfelt, 1984) in responding to environmental threats, whatsoever, (Barney, 1997) by protecting its assets. Therefore IS security policy becomes a critical device for protecting information systems.

A good and effective security policy reflects strategic priorities and assets of the organization (Kabay, 1999). Therefore ISPD process should suitably synchronize ISP with the organizational processes. Hence, for an effective security policy it should be considered in terms of business purpose, goals and vision of the organization as a wholesome holistic approach (Poulymenakou and Holmes, 1996). Therefore, an ISPD approach should reflect following criteria to reflect that it meets the syncing with organizational needs principle.

1. Synchronized with the organizational objectives
   - Legal requirements
   - Cultural and ethical practice
2. Aligned with the Critical Success Factors
   - Business focus (Product leadership or price leadership)
   - Industry it operates in

Principle 2: Organizational Adaptability

This principle explicates that organizational adaptability is a must feature for the organizations aiming to have high security strategy. Acquiring a security competence in terms of managing all the issues, and developing and writing security policy are often seen as challenge which organizations fail in acquiring or adapting to the security need. Therefore, acquiring a new competence, particularly by an existing organization is encountered as significant impediment in meeting security need.

The concept of adaptable organization founds on the features of flexible organization and learning organization. A flexible organization enables organizations to prepare better in changing and unpredictable environment (Dreyer and Gronhaug, 2004). Flexible organizations reflect preparedness to meet the IS security challenges recognized as significant organizational need. With flexibility, organizations can continuously create right kind and range of resources coordination (Sanchez 1997). Dynamic contingency theory explicates flexibility can be achieved by integrating, reconfiguring and developing organizational resources and competences to address uncertainties and complexities (Fredricks, 2005; Boyle 2006) and an ability to control the changing and unpredictable business environment (Eppink, 1978; Krijnen, 1979; Aaker and Mascarenhas, 1984; Volberda, 1998). Theory of organizational learning has been receiving increasing attention (Dodgson, 1993) especially in responding to rapid changes, thus to effectively sustain their existence in the fast changing world (Hannan and Freeman, 1984; Kenny 2006).

An adaptable organization will form task force or temporary team by involving representative sample and intercompany learning for better integration (Kabay, 1999). Hence, an ISPD approach should reflect following criteria to reflect that it meets the adaptable organization principle.

1. Formation of task force
    - Representation from top management, IT and security
    - Representation from all impacted department
2. Flexibility in acquiring security competence
    - Recruitment of professional – security policy
    - Competence development pertaining to security matter

Principle 3: Users’ involvement

Top down approach and user resistance to change is observed as the primary reason for the failure of various technical projects (Hirschheim and Newman, 1988). Treating ISP development principally as only a technical process could be a recipe for disaster (Hirshheim and Newman, 1991). Thus treating security policy development a technical matter and not a social issue causes various problems. Lack of user involvement causes low understanding of the security need leading inadequate importance of the security policy. Since, often, employees at operational level are aware better of the critical business aspects than the top management, lack of user involvement in this case leads to a security policy with inadequate focus on critical business aspects.

The sociotechnical approach is founded on user participation during development phase. User participation works as a tool for improving users' perception about the significance of IS security measures (Spear and Barki, 2010). Buy in theory explains that user participation bring positive attitude of users in adhering to policy. The change in attitude is achieved by facilitating the feeling of belongingness to security policy ensured by participation. Socio-technical approach propagates decentralized and delegated decision making, which extends the sense of belongingness to users in developing and implementing policy. System quality theory explains that participation ensures thorough understanding of business needs and a comprehensive attention to security needs, which consequently enhances quality of security policy. The entire exercise of participation in assessing business need facilitates alignment of security policy with the environment organizations operate in. Such participation also ensures early evaluation of security policy at development stage and users also get to know the exact picture what entails implemented security policy, critical for eventual success (Szajna and Scamell, 1993).

According to the view of Mumford and Weir (1979), technical professionals, for security policy security professionals, should regard themselves as facilitator supporting the users in defining desirable and sustainable security policy for the users' environment. Organizations use formal training for the development of competencies that are critical to the achievement of purpose of the security policy (Hayes 2006). User education is significant tool for an effective security policy (Madnick, 1978). Organizations rely on users, through training, in exercising their skill to identify and resolve problems, introduce changes in work methods, and take responsibility of quality, in this case it is responsibility of complying with security policy (Pfeffer 1998). An ISPD approach should reflect following criteria to reflect that it meets the users' involvement principle.

1. Representation of users in task force
   - All relevant departments are involved
   - Participation in requirements elicitation exercise
2. Provision for required training, awareness and communication
   - Training provisions according based on users need
   - Communication strategies aiming to change users behavior

Principle 4: Top management commitment

The principle focuses on involving top management into the entire process of ISP formulation and implementation. It is critical to involve top management, because lack of top management commitment leads to three most pressing issues that hinder the success and effectiveness of security policy. Lack of top management commitment to security policy causes low priority activity. This further leads to lack of deploying needed resources and lack of overall motivating atmosphere within the organization. Security policy development and implementation needs immense resources in terms of time of employees and top management, new competence development for handling security issues, and financial resources. Lack of overall motivation leads to low adherence to security policy by the users.

Expectancy theory of commitment explicates that decision makers can be influenced by the subjective utility of allocating resources by anticipating value of goal attainment from security policy (Brockner, 1992). This helps management in understanding the value of allocating required resources, probability of goal attainment, cost-benefit analysis that drives the commitment (Newman and Sbherwal, 1996). A consensus among the decision makers for the need of an effective security policy will make a positive impact towards the involvement of top management (Newman and Sabherwal, 1996; Hayes, 2006).

Commitment from the management has two explicit implications. First, a committed management will deploy appropriate resources required for the policy formulation, development and implementation, and second, sincere involvement of management is seen as motivation and relevance by employees in adhering to security policies. Therefore, an ISPD approach should reflect following criteria to reflect that it meets the top management commitment principle.

1. Management representation
    - Task force for security policy
    - Meeting related to security policy formulation and implementation
2. Resource allocation
    - For all the needed activities (training, communication, meeting, etc)

- For acquiring security competence (new employee or training of an existing employee[s])

Principle 5: Cogent policy

Employees comply with security policy if they find it to be useful for the organization and easy to use which does not challenge their cognitive and physical limitations. Although users' involvement principle ensures that users are involved in requirement engineering and they are trained and educated in adopting security policy. Nevertheless, this does not necessarily imply that language and technicality of security policy is addressed and users easily understand the policy. In an empirical study employees had complaint about highly technical language of the policy, which is difficult to interpret and understand, consequently employees fail in complying with these policies (Puhakainen and Siponen, 2010). The eventual success of security policy lies in reading, understanding and complying with the policy.

Performance expectancy theory and effort expectancy theory together explain that user finds security policy useful in achieving her/ his job performance on the one hand and on the other hand security policy should be easy to use. Policy formulation should include human characteristics of the organization. In a recent research users express their willingness to participate in the defining, testing, implementing, phase of the policy development (Ferreira *et al.* 2010).

Security policy is a technical document, writing a security policy document should be dealt by professionals. As mentioned in business need principle, organizational culture and ethics are critical issues; these issues can be addressed if users are involved in writing the document. This approach of writing security policy will also address the issue of evaluation during development phase. A security policy development approach should reflect following criteria to reflect that it meets the users' involvement principle.

1. Participatory approach in policy writing,
   - Involvement – users' representatives
   - Evaluation of policy during development phase
2. Policy written by expert / professional
   - Professional hired or contracted, who has policy writing competence and experience
   - Involvement of the professional from the initial stage

Table 2: Essential principles

Principles	Issues	Theory	Criterion
Syncing with organizational need	One standard policy cannot serve different business needs as Businesses are different due to nature, industry strategy, business objective, organizational design, culture, and legal requirements,	Resource-based view	1. Synchronized with the organizational objectives • Legal requirements • Cultural and ethical practice 2. Aligned with the Critical Success Factors • Business focus (Product leadership or price leadership) • Industry it operates in
Top management commitment	Security policy is not the priority Lack of resources • Human resource • Capital or recurring Lack of overall motivation • Security professionals • Employees at large	Expectancy theory of commitment	1. Management representation • Task force • Meeting 2. Resource allocation • For all the needed activities (training, communication, meeting, etc) • For acquiring security competence (new employee or training of an existing employee)
Organizational adaptability	Organizations are not prepared to adapt to	Dynamic contingency	1.Formation of task force Representation from top

	dynamic environment Organizations fail in implementing effective security policy Organizations fail in creating need for security professional Organizations fail in acquiring competence required for addressing security needs	theory	management, IT and security Representation from all impacted department 2. Acquiring security competence • Recruitment of professional – security policy • Competence development of employees
Users' involvement	Lack of user involvement causes low significance for security policy Lack of understanding of the security policy Security policy fails to cover all critical business aspects Policy does not meet expectations of the users	Sociotechnical view	1. Representation of users in task force • All relevant departments are involved • Participation in requirements elicitation exercise 2. Provision for required training and communication • Provision for training according to users need • Provision for communication strategies aiming to change users behavior
Cogent policy	A complicated and / or technical policy is difficult to understand Difficult to understand policy challenges • Human limitations • Causes pressure in regular job performance Results in low adherence	Performance expectancy theory and effort expectancy theory	1.Participatory approach in policy writing, ensuring language acceptable and understandable to users 2.Policy written by expert, ensures all the critical aspects are covered and policy is appropriately formulated

5. Analysis of the extant ISPD literature

Evaluation:

Based on the essential principles and their respective criteria above, this section evaluates and analyzes existing ISP methods. These ISP methods will be evaluated into three different categories, 1) none of the criteria is present in the approach, 2) out of two, only one criterion is present in the method, and 3) will represent that both the criteria are present in the method. For detailed evaluation kindly refer to appendix 1.

i) Unique business need

This is the principle which received most attention by the extant ISP methods. Of the 42 analyzed methods, 10 methods meet both of the criteria of this principle, while 17 meets only one of the criteria.

ii) Organizational adaptability

Formulation and implementation of security policy entails changes in organization that necessitates adaptation to these changes for successful security policy. This is another principle which lacks room in the founding of ISP methods. Only two methods, Karyda *et al.* (2003) and Karyda *et al.* (2005), meet the criteria of this principle, while only 7 other methods meet only one of the criteria of this principle.

iii) User's involvement

Application of Socio-technical theory for the success of technical solutions has been widely discussed and researched to involve end users. This is quite reflective in the analysis done in the section above. This principle has also received good attention by the information security regime. Six methods meet both the criteria of this principle, while 25 methods meet only one of the criteria.

iv) Top management commitment

This is another principle which does not find adequate space in the extant methods. Only the paper of Kadam (2007) meets all the criteria of this principle. While only 13 other methods meet only one of the criteria. Although, this is one of the most discussed issues but lacks proper attention.

v) Cogent policy

Technical and clumsy language of security policy has been the significant impediment in the eventual success of security policy. This principle does not get appropriate attention in the ISP methods while user's involvement principle in formulating security policy has found relatively good attention. Principle of users' involvement and principle of cogent policy complement each other. Cogent policy cannot be achieved without involving users, but this principle comes in role after requirement gathering which is dealt by users' involvement principle. None of the methods meet both the criteria of this principle, while 10 methods meet one of the criteria of this principle.

To summarize the results of the analysis, none of the extant security methods meet all five principles for ISP development methods. This inadequacy entails a gap that needs to be addressed by future research. In the next section, we describe directions for future research aimed at addressing these six principles.

6. Discussion

We analyze that none of the extant ISP methods are based on all essential principles. Therefore, there is a need of immediate attention to develop an ISP method that is comprehensive and founded on all the five principles. Henceforth, by focusing on the five essential principles we suggest implications for research and implications for practice.

Implications for research:

(1.) First avenue for future research is based on the five principles and their respective issues. The principles discussed are mutually exclusive and collectively exhaustive. This means that all the principles are separate and taken together solve the problem without leaving gap. Therefore we believe that it will be interesting to see how much each principles show exclusivity and does leave gap in solving problem. This research can focus on all five principles individually.

(2.) This can be to develop a comprehensive ISP method by following design science approach. Since none of the existing ISP methods meet the criteria of essential principles, therefore, designing ISP method based on these principles would be interesting.

(3.) Another avenue can be to develop a theory of effective policy model. The need for a comprehensive ISP method can be the motivation for this proposed theory. This research avenue can be based either on quantitative research approach or qualitative approach.

Implications for practice: We convincingly recommend to practitioners for designing ISPD method founded on the principles discussed in this paper. Since these principles are mutually exclusive and collectively exhaustive, we therefore suggest applying all the principles together for an optimum result.

a) Unique business need: Companies should formulate their own security policy due to differing needs. Companies have different information and knowledge assets based on their industry, strategy, leadership style, atmosphere and structure of the company, culture and ethical practices. To focus on all these issues appropriately we recommend focusing on participatory requirement gathering exercise. Thus focus on all the relevant aspects of internal and external factors and match with the operational issues of the companies that could be unique in nature.

b) Top management commitment: The most prominent way of achieving this goal is by evaluating the risk threats. Risk analysis is a communicative tool for laying down the foundation for the need of ISP (Baskerville, 1991). This exercise is mainly conducted by a group of IT experts, risk analysts and top management.

c) Organizational adaptability: Being adaptable, organizations can form task force that consists of top management, related professionals / experts / consultants and representatives from different departments / groups. This team will carry out all the necessary activities such as requirement engineering, policy writing, implementing, training, campaigning, monitoring, evaluating and documenting their learning work. An adaptable organization will also acquire new competence for managing security and writing security policy, training, and understanding end users' need. These can be efficiently performed by experts. Organizations based on their requirements and size can determine whether to create a new role by hiring a new professional / expert or to develop in house competence.

d) Users' involvement: All the major activities are performed by the users' representatives, while professionals / experts / consultants play mainly the role of facilitator and top management representation ensures criticality of the issue and drives motivation in the organization *per se*.

Involvement also include training of users based on their need, and awareness and communication strategies aiming to creating a right kind of lasting security culture.

e) Cogent policy: This principle ensures that users' involvement continue during the writing and evaluating phases of security policy. In achieving the purpose of lucid and simple security policy easy to understand that does not challenge users' cognitive and physical abilities, this phase of writing and evaluating must be clearly supported by expert.

7. Conclusions

ISP is the critical foundation for protecting information systems, yet a systematic methodology for delivering ISPs remains a pressing issue. In this paper, we put forth meta-theoretical approach for understanding fundamental characteristics of ISPD process, and thus suggest essential principles for designing ISP methods. These essential principles were: 1) ISP development methods must facilitate formulation of ISPs that meet unique business need, 2) ISP methods will not realize the benefits if do not get top management commitment, 3) Organizations intending to have ISP should be adaptable to the requirements of ISPD, 4) ISPDM should focus on involving users, and 5) ISPDM should be founded on developing easy to understand and acceptable policy. We demonstrated that none of the extant ISP methods meet all the essential principles put forth in this paper. Therefore, we called for a further research for designing ISPD method that meets these five principles. By advancing research in this field we believe that scholars can develop a comprehensive ISP method that can formulate and implement effective ISPs and thus address a pressing issue in the field of IS security.

References

Aaker, D.A. and Mascarenhas, B. (1984). The need for strategic flexibility, *The Journal of Business Strategy*, 5 (2), 74 – 82.

Abrahamsson, P., J. Warsta, et al. (2003). New directions on agile methods: A comparative analysis, *International Conference on Software Engineering* (ICSE25), Portland, Oregon.

Abrams, M.D. & Moffett, J.T. (1995). A Higher level of computer security through active policies, *Computer & Security*, 14(2), 147-157.

Akers, R. L. and Sellers, C. S. (2004). Criminological Theories: Introduction, Evaluation, and Application. Fourth Edition. Los Angeles, CA: Roxbury Publishing

Anderson, R. (1996), A Security Policy Model for Clinical Information Systems, 1996 IEEE Symposium on Security and Privacy.

Anderson, J.G. (2000). Security of the distributed electronic patient record: a case-based approach to identifying policy issues, *International Journal of Medical Informatics*, 60 (2) 111-118.

Arnesen, D.W. and Weis, W.L. (2007). Developing and effective company policy for employee internet and email use, *Journal of Organizational Culture, Communications and Conflict*, 11(2), 53 – 65.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage, *Journal of Management*, 17, 99-120

Barney, J. (1997). Gaining and sustaining competitive advantage, Addison-Wesley Pub. Co.

Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security, *European Journal of Information Systems*, 1(2), 121 – 131.

Baskerville, R. & Siponen, M.T. (2002). An Information Security Meta-policy for Emergent Organizations, *Journal of Logistics Information Management,* special issue on Information Security, 5(6), 337-346.

Bensaou, M., and Earl, M. (1998). The Right Mind-set for managing information technology, *Harvard Business Review*, (September – October 1998), 119 – 128.

Boswell, A. (1995). Specification and validation of a security policy model, *IEEE Transaction on Software Engineering*. February, 21(2), 63-68.

Boyle, T.A. (2006). Towards best management practices for implementing manufacturing flexibility. *Journal of Manufacturing Technology Management*, 17 (1), 6-21.

Brand, M. (2006). Managing Information Security Complexity, *Australian Information Security Management Conference*, Security Research Centre Conferences, Edith Cowan University, Research Online

Brewer, D.F.C. & Nash, M.J. (1989). The Chinese Wall security policy, 1989 IEEE Symposium on Security and Privacy.

Brockner, J. (1992). The Escalation of Commitment to a Falling Course of Action: Toward Theoretical Progress, *Academy of Management Review*, 17(1), 39 - 61.

Chua, W.F. (1986). Radical Developments in Accounting Thought. Accounting Review. 61(5), 583-598.

Coles-Kemp, L. and Theoharidou, M. (2010). Insider Threat and Information Security Management, in Insider Threats in Cyber Security, *Advances in Information Security* (Springer), 49, 45-71

Corby, M.J., (1999), Policy development. In: M. Krause and H.T. Tipton (eds): Handbook *of Information Security Management*, CRC Press LLC, FL, USA, pp. 403-422.

Corby, M.J (2007). Policicy Development (Chapter 4-4-1).Krause,M. and Tipton,H.F. Handbook of Information Security Management. Publisher: CRC Press LLC.

David, J. (2002). Policy enforcement in the workplace, *Computers & Security*, 21(6), 506-513.

Dhillon, G. and Torkzadeh, G. (2006). Value Focused Assessment of Information System Security in Organizations. *Information Systems Journal*, 16(3). 293 – 314.

Dhillon, G. (2001). Information Security Management: Global Challenges in the New Millennium, Idea Group Publishing.

Dodgson, M. (1993), Organizational learning: a review of some literatures, *Organization Studies*, 14(3), 375 - 394.

Dreyer, B. and Gronhaug, K. (2004). Uncertainty, flexibility and sustained competitive Advantage, *Journal of Business Research*, 57(5), 484 - 494.

Eppink, D.J. (1978). Managing the Unforeseen: A Study of Flexibility. Dissertation thesis. Ermelo: Administratief Centrum.

Ferreira, A., Antunes, L., Chadwick, D. , Correia, R. (2010). Grounding information security in healthcare. *International Journal of Medical Informatics* 79 (2010) 268-283.

Fredericks, E. (2005). Infusing flexibility into business-to-business firms: a contingency theory and resource-based view perspective and practical implications, *Industrial Marketing Management*, vol. 34 no. 6, pp. 555 - 565.

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

Garner, R. T & Rosen, B.(1967). Moral Philosophy: A Systematic Introduction to Normative Ethics and Meta-ethics.

Good, I. (1966). A note on Richard's Paradox. Mind, New Series, 75, No. 299, p. 431.

Gonjalez, J. and Sawicka, A. (2002). A framework for human factors in information security, presented at the 2002 *WSEAS International Conference on Information Security*, Rio de Janerio, 2002.

Gregor, S. and Jones, D. (2007). The anatomy of a Design Theory, JAIS, (8: 5), Article 2, 312 – 335.

Habermas J (1984) The theory of communicative action – reason and the rationalisation of society (Vol I), Beacon Press, Boston, MA.

Habermas J (1987) The theory of communicative action – the critique of functionalist reason (Vol II), Beacon Press, Boston, MA, USA.

Hannan, M.T. and Freeman J. (1984). *Structural* inertia and organizational change, American Sociological Review, 49(2) 149-164.

Hare, R. M. (1981). Moral Thinking : Its level, method, and point. Oxford: Clarendon Press.

Hayes, J. (2006). The Theory and Practice of Change Management, Second edition, Palgrave Macmillan.

Hayes, J. (2010). The Theory and Practice of Change Management, Third edition, Palgrave Macmillan.

Hirschheim, R.and Newman, M. (1988). Information Systems and User Resistance: Theory and Practice, *The Computer Journal,* 31(5), 398-408.

Hirschheim, R. and Newman, M. (1991). Symbolism and Information Systems Development: Myth, Metaphor and Magic, *Information Systems Research*, March, 2(1), 29-62.

Hirchheim, R., Klein, H.K., Lyytinen, K. (1995) Information Systems Development and Data Modelling : Conceptual and Philosphical Foundations. *Cambridge University Press*.

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

Ishikawa, K., (2000), Health data use and protection policy; based on differences by cultural and social environment. International Journal of Medical Informatics, 60(2), 119-125.

ISO 27001.

Iivari, J. & Kerola, P. (1983). A Sociocybernetic framework for the feature analysis of information systems design methodologies. In T.W. Olle, H.G. Sol, C.J. Tully (eds.), Information Systems Design Methodologies: A Feature Analysis, 87-139, North-Holland, Amsterdam.

Iivari, J., Hirschheim, R. (1996), Analyzing Information Systems Development: A Comparison and Analysis of Eight IS Development Approaches. Information Systems. 21(7), 551-575.

Kabay, M.E. (1999). The INFOSEC Year in Review, Information Security Magazine (Dec 1999)

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

Kant, I. (1993). The moral law: groundwork of the metaphysic of morals. Routledge, London, UK.

Karyda, M., Kiountouzis, E. and Kokolakis, S. (2005). Information Systems Security Policies: A Contextual Perspective, *Computers and Security*, 24, 246 – 260.

Karyda, M., Kokolakis, S., Kiountouzis, E., (2003), Content, Context, process analysis of IS security policy formulation. Proceedings of the IFIP TC11 18th International Conference on Information Security (SEC2003), May 26-28, Athens, Greece, 145-156.

Kenny. J. (2006). Strategy and the learning organization: a maturity model for the formation of strategy, *The Learning Organization: An International Journal*, 13(4), 353 - 368.

Klein H.K. & Hirschheim, R., (2003), Crisis in the IS Field? A Critical Reflection on the State of the Discipline. Journal of the Association for IS, Volume 4 Article 10 October.

Krijnen, H.G. (1979). The flexible firm, *Long Range Planning*, 12(2), 63 – 75.

Lindup, K. R., (1995), A New Model for Information Security Policies. *Computer & Security*, 14(8), 691-695.

Ma, Q., Schmidt, M.B., and Pearson, J.M. (2009). An integrated framework for Information security management, *Review of Business,* (October 2009), 30(1), 58 – 69.

Madnick, S. E. (1978). Management Policies and Procedures Needed for Effective Computer Security*, Sloan Management Review*, (20:1), 61 – 74.

Marcinkowski, S.J. and Stanton, J.M. (2003). Motivational aspects of information security policies, IEEE International Conference on Systems, Man and Cybernetics, 3, 2527 - 2532

Maynard, S.B. and Ruighaver, A.B. (2006). What Makes a Good Information Security Policy: A Preliminary Framework for Evaluating Security Policy Quality, 5th Annual Security Conference, Publisher: The Information Institute (Las Vegas).

Mumford, E. and Weir, M. (1979) Computer Systems in Work Design - The ETHICS Method, Associated Business Press.

Newman, M. & Sabherwal, R. (1996). Determinants of Commitment to information Systems development: a longitudinal investigation, *MIS Quarterly*, 20(1), 23-54

Olnes, J. (1994). Development of Security Policies, *Computers & Security*, (13), 628-636.

Orlikowski , W.J. and Robey, D. (1991). Information Technology and the Structuring of Organizations. *Information Systems Research*, 2(2), 143-169.

Palmer, M.E., Robinson, G., Patilla, J, & Moser, E.P. (2001). Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age, *Information Systems Security*, 10(2), 1-15

Penrose, E. T. (1959). The Theory of the Growth of the Firm. New York: John Wiley.

Poulymenakou, A. and Holmes, A. (1996). A contingency framework for the investigation of information systems failure, *European Journal of Information Systems*, 5, 34 – 46.

Puhakainen, P. and Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study, *MIS Quarterly*, 34(4), 757-778.

Sanchez, R. (1997). Preparing for an uncertain future: Managing organizations for strategic flexibility, *Int. studies of Mgt. & Org*. (Summer 1997), 27(2), 71 – 94.

Schultz, E.E., Proctor, R.W., Lien, M., and Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods, *Computers and Security*, 20(7), 620 – 634.

Selznick, P. (1957). Leadership in administration, Harper & Row (New York).

Siponen, M.T. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods, *Information and Organization*, 15, 339 – 375.

Spears, J. L. and Barki, Henri. (2010). User Participation in Information Systems Security Risk Management, *MIS Quarterly*, 34(3), 503-522.

Thompson, J.D. Copyright © (1967). Organizations in action: Social science bases of administrative theory, Mc Graw-Hill book company.

Trompeter, C.M. and Eloff J.H.P. (2001). A framework for the implementation of socio-ethical controls in information security, *Computers & security*, 20, 384 – 391.

Volberda, H.W. (1998). Building the Flexible Firm: How to Remain Competitiveness. New York: Oxford University Press Inc.

Walls, J.G. , Widmeyer, G.R., El Sawy O.A. (1992). Building an Information System Design for Vigilant EIS. *Information Systems Research* , 3(1), 36-59.

Warman, A.R. (1992). Organizational computer security policy: the reality, *European Journal of Information Systems*, 1(5), 305-310.

Wen, H.J. (1998). Internet computer virus protection policy, *Information management & computer security,* 6(2), 66 – 71.

Wernerfelt, B. (1984). A resource-based view of the firm, *Strategic Management Journal*, 5, 71–80.

Whitman, M.E. (2008). Chapter 6: Security Policy: From Design to Management, pp 123 – 151. In Information Security: Policies, Processes and Practices, edited by Straub, Detmar W. and Goodman, Seymour, Publisher: M.E. Sharpe (New York).

Whitman, M.E., Townsend, A.M., and Aalberts, R.J. (2001). Chapter II: Information systems security and the need for policy, pp 9 – 18. Information security Management: Global Challenges in the New Millennium edited by Gurpreet Dhillon, Idea Group Publishing.

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

Wood, C.C. (1995). Writing InfoSec Policies, *Computer & Security*, 14(8), 667 674.

Yusufovna, S.F. (2008). Advanced security policy implementation for Information Systems, 2008 *International Symposium on Ubiquitous Multimedia Computing*, Downloaded from IEEE Xplore.

Appendix 1

Evaluation criteria:

Based on the essential principles and their respective criteria above, this section evaluates and analyzes existing ISP methods. These ISP methods will be evaluated into three different categories -, 1 and 2. Category - will represent that none of the criteria is present in the approach, while 1 will represent that out of two, only one criterion is present in the method, and 2 will represent that both the criteria are present in the method.

Category	Evaluation
None of the criteria	-
One of the criteria	1
Both the criteria	2

Evaluating the literature:

	Literature on security policy approach	Unique Business Need	Top Management Commitment	Organizational Adaptability	Users' involvement	Cogent Policy
1	Karyda *et al.* (2003)	1	1	2	1	-
2	Karyda *et al.* (2005)	2	1	2	1	-
3	Kadam (2007)	1	2	-	2	1
4	ISO 27001	2	1	1	1	-
5	Whitman *et al*. (2001)	2	-	-	1	1
6	Ølnes (1994)	1	-	-	1	1
7	Höne and Eloff (2002)	1	1	-	2	1
8	Gaunt (1998)	-	-	-	2	-
9	Simms (2009)	2	-	-	1	-
10	Ferreira *et al.* (2010)	-	-	-	2	1

11	Ølnes and Maillot[1]	2	-	-	-	-
12	Kabay (1993)	-	1	1	2	-
13	Whitman (2008)	1	-	-	1	-
14	Madnick (1978)	1	1	1	1	-
15	Park *et al.* (2010)	1	-	-	1	-
16	Wood (1996c)	-	-	-	-	1
17	Abrams and Moffett (1995)	-	-	-	-	-
18	Anderson (1996)	1	-	-	-	-
19	Wen (1998)	1	-	-	1	-
20	Corby (1999)	1	-	-	1	1
21	Wood (1995)	1	1	1	-	-
22	Boswell (1995)	-	-	-	-	-
23	Brewer and Nash (1989)	-	-	-	-	-
24	David (2002)	-	-	-	-	-
25	Ishikawa (2000)	-	-	-	-	-
26	Warman ((1992)	1	1	-	1	-
27	Baskerville and Siponen (2002)	2	-	1	1	-
28	Trompeter and Eloff (2001)	2	-	-	1	-
29	Ma *et al.* (2009)	2	1	-	1	-
30	Palmer et al. (2001)	1	1	-	1	-
31	Höne and Eloff (2002)	1	1	-	1	1
32	Gonzalez and Sawicka (2002)	-	-	-	1	-
33	Schultz *et al.* (2001)	-	-	-	1	-
34	Brand (2006)	2	-	-	-	-
35	Maynard and Ruighaver (2006)	2	-	1	1	1
36	Dhillon (2007)	1	-	-	1	-
37	Dhillon and Torkzadeh (2006)	-	1	1	2	-
38	Lindup (1995)	-	-	-	1	-
39	Arnesen and Weis (2007)	-	-	-	1	-
40	Eloff and von Solms (2000)	-	-	-	-	-
41	Coles-Kemp and Theoharidou (2010)	1	1	-	1	1
42	Yusufovna (2008)	1	-	-	1	-

[1] http://publications.nr.no/paper030696.pdf

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org