2011

Stakeholders in security policy development

S B. Maynard
University of Melbourne

A B. Ruighaver
Deakin University

A Ahmad
University of Melbourne

10.4225/75/57b546fecd8c6
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

STAKEHOLDERS IN SECURITY POLICY DEVELOPMENT

S. B. Maynard 1, A. B. Ruighaver 2, A. Ahmad [3]
[1,3] Department of Information Systems, The University of Melbourne, Victoria, 3010
[2] School of Information Systems, Deakin University, Melbourne, Australia
[1] seanbm@unimelb.edu.au, [2] tobias@deakin.edu.au, [3] atif@unimelb.edu.au

Abstract
The Information Security Policy (ISP) of an organisation is expected to specify for employees their behaviour towards security, and the security ethos of the organisation. However, there are a wide range of opinions and expertise that should be considered by organisations when developing an ISP. This paper aims to identify the stakeholders that should be utilised in an ISP development process and how this may differ based on organisational size. The research identifies from literature nine stakeholder roles that are suggested to be required in an ISP development process. Contextual interviews are then used to validate these nine stakeholder roles from a practical perspective.

Keywords
Security Policy, Stakeholders, Information Security Management

INTRODUCTION

Organisations are continually having to protect themselves from a myriad of security threats which have been shown to be on the increase (Dhillon 2007). Hu et al. (2007) suggest that an organisation, whilst having technical security controls, needs to also have good managerial practices regarding security, in particular having a good information security policy (ISP). "Undoubtedly the singularly most important of these controls is the information security policy" (Hone & Eloff 2002, p.402). An ISP defines how information and related assets of an organisation are protected from various threats that may impact on the accuracy, availability, integrity and confidentiality of an organizations' information (Doherty et al. 2009).

One of the concepts of ISP development that is generally agreed upon by researchers is the need to involve multiple perspectives (Warman 1992; Szuba 1998; Swanson 1998; Dhillon & Torkzadeh 2001; Tudor 2001). Having multiple stakeholders involved in ISP development will help to produce a more balanced policy that will be applicable to the diverse stakeholders of the organisation, whilst still defining the security agenda of the organisation.

Given the importance of ISP to an organisation and that multiple stakeholders should be involved in policy development; two questions arise a) which stakeholders should be involved in development and b) when should stakeholders be involved with development. This research aims at answering only the first of these questions: which stakeholders should be involved in development. The second question will be dealt with in future research.

In order to determine which stakeholders should be involved in ISP development a conceptual review of the literature was undertaken. This was followed up by a number of contextual interviews with information security experts to determine a practical perspective. This research reports on these procedures.

METHODOLOGY

The purpose of this paper is to investigate which stakeholders in organisations should be involved with the ISP development process. Initially a conceptual study was undertaken that identified nine stakeholder roles that are discussed extensively in the literature. Next, a series of contextual interviews (as defined by Holtzblatt et al. 2005) were undertaken to determine which stakeholders practitioner experts thought were important in ISP development.

Experts were selected for this study based on the amount of experience they had in information security and in particular whether they conducted ISP development. Identification of experts was obtained through contacts provided by colleagues and through calling organisations to talk to information security managers. The full process for this was to identify a security expert, to then make telephone contact, ascertain their suitability and interest and to then conduct an interview. All interviews were recorded digitally, were transcribed and analysed to gain an insight of their perceptions regarding stakeholder roles in policy development. The interview process was conducted until saturation was reached. Table 1 summarises the experts interviewed.

Table 1: Contextual Interview Experts

Interviewee	Job Title	Industry Sector	Years of Security Experience
Fred	Manager IT Security	Supply Chain	5 years
Greg	Security Analyst	Supply Chain	4 years
Hilda	Security Specialist	Automotive	7+ years
Inga	Security Manager	Financial Services	4 years

Participants were asked two main open ended questions: "How are ISPs developed in your organisation, including who is involved with the development?" and "Which stakeholders should be involved with the development, implementation and evaluation of security policies?". The second question was asked later in the interview, and elicited similar stakeholders to those previously identified in their description of policy development.

In the following section each of the stakeholder roles will be described, and the results of the contextual interviews will be presented.

DEFINING STAKEHOLDERS IN ISP DEVELOPMENT

In ISP development research, a number of different stakeholders have been suggested. These are summarised in Table 2. This table contains two columns; the first column gives a synonym for the stakeholder type and the second column list the stakeholders of that type. In this section the stakeholder roles will be discussed in detail and the results of the contextual interviews will be presented.

Table 2: Stakeholder roles suggested in the literature

Synonym	Stakeholder
Executive Management	Top Management (Abrams & Bailey 1995) Managers (Baskerville 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 1988; Warman 1992; Leinfuss 1996; Swanson 1998) Computer Users (Abrams & Bailey 1995) User Community (Robinson 1997) Data Entry Staff (Szuba 1998) Data Processors (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 1988)
Legal & Regulatory	Legal Department (Robinson 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)

Synonym	Stakeholder
	Security People (Anderson Consulting 1999) Information Security Team (Diver 2007)
Public Relations	Public Relations (Anderson Consulting 1999)

From Table 2 it can be seen that many researchers discuss which personnel should be involved with the development of ISP (Warman 1992; Szuba 1998; Swanson 1998; Dhillon & Torkzadeh 2001; Tudor 2001), or the stakeholders who should be involved with security in general (Baskerville 1988). Each stakeholder role may have involvement with ISP development at different levels, at different times and may have differing opinions about the policy. Thus, it is important to include all possible stakeholders in the development process. It is important to note here, that these are stakeholder roles, as opposed to jobs, and as such a particular individual may take on more than one role. For instance in a small organisation a single IT manager may be employed and it would be likely that they would take on the roles of *ICT Specialist* and *Security Specialist* during the ISP development lifecycle.

User Community

The *User Community* for any organisation consists of individuals (and groups of individuals) who carry out a variety of diverse functions. ISP literature tends to group the *User Community* under a number of banners, the most popular being "end users" (Baskerville 1988; Warman 1992; Leinfuss 1996; Swanson 1998). Other terms used in the security literature include Computer Users (Abrams & Bailey 1995), User Community (Robinson 1997; Diver 2007), Data Entry Staff, Data Processors and Information Collectors (Szuba 1998).

Robinson (1997) and Diver (2007) suggest that the *User Community* needs to be represented well in the development effort to ensure that the multidisciplinary nature of organisations is intrinsically integrated in the ISP. Furthermore, Szuba (1998) suggests that having involvement of the *User Community* in the development process results in "buy-in" in the development process creating a sense of ownership of the ISP. Diver also states "it can be useful to work with users to determine how successful current security policy is, and thereby determine how the policy may need to be changed to make it more usable for your target audiences" (Diver 2007, p. 17).

Whatever the concerns of the users may be, the consensus in the literature is that end user, or *User Community* consideration in the ISP development process is extremely important for a number of reasons, including the fact that so many security incidents are caused, intentionally or unintentionally, by employees within the organisation (Baskerville 1988; Warman 1992; Leinfuss 1996).

Legal & Regulatory

One of the main compelling reasons that organisations have for developing ISP is to mitigate the various security risks that the organisations faces (Doherty et al. 2009). Essentially they are protecting themselves from people who want to exploit its resources and who, in doing so, may break laws, or perhaps act inappropriately in the organisations eyes. As a result, many organisations obtain legal advice to ensure that their policy is a legally binding document (Robinson 1997; Szuba 1998) and is enforceable (Diver 2007). Furthermore, regulatory requirements of the State (Baskerville 1988), or of industry bodies (Anderson Consulting 1999) must be adhered to and this may need to be reflected in the policy. For example many countries have introduced legislation aimed at protecting the privacy of individuals, or to attempt to make spam mail illegal. For these reasons, the inclusion of *Legal & Regulatory* personnel in the ISP development process is paramount.

ICT Specialists

The *ICT Specialist* is usually one of the driving forces of the ISP development process. As a result, the *ICT Specialist* role is highly represented in the ISP development literature. In practice the *ICT Specialist* may come from a number of varying roles dealing with the management of an organisation's computing infrastructure. These roles include (but are not limited to) Technical Computer Specialists (Warman 1992; Diver 2007), the System Designer (Baskerville 1988), IT Specialists (Robinson 1997), the System Administrator (Swanson 1998), IS Professionals (Anderson Consulting 1999), IT Department personnel (Woodward 2000).

The use of one or more these stakeholders in the development is critical as they have technical knowledge of the systems that the ISP is being designed to protect as well as security knowledge of these systems (Robinson 1997; Swanson 1998; Anderson Consulting 1999; Diver 2007). Traditionally, security policies tend to be developed from the bottom up, and this process is usually driven from the IT area of the organisation. As such, policies developed in this manner tend to have a very technical focus, rather than a focus on the organisation as a whole. Woodward (2000) found that problems occur if the development process is purely driven from the IT Department. These problems occur as the views of security within the IT department may differ from those of

management or other stakeholder roles. Warman (1992) shares this view and found that technical computer specialists, whilst actively involved in the development process, should not be the only driving force being the development of policy. Including other stakeholders in the development and quality assessment process should reduce the impact that ICT Specialists have on the overall development, use and evaluation of the organisations ISP.

Security Specialists

The *Security Specialist* role within an organisation has often been played by someone in IT as an adjunct to their main organisational role. More frequently, however, medium to large organisations are employing people in roles focusing on protecting the organisation's information, and on the development of security policies. The use of people in these roles in the ISP development process ranges from the management of the complete process, through to consulting them for ideas and advice regarding security initiatives. This stakeholder role should be intimately familiar with security matters, but may not know about the full inner workings of the computer systems and communications within the organisation. Often this stakeholder will be placed in charge of the ISP development process (Diver 2007).

Human Resources

In an ISP development lifecycle *Human Resource* involvement is paramount to ensure that the policy meets standard organisational practices. The focus of *Human Resources* will be on the consistency of the ISP with the organisational standards, equity of the policy and on training. They will ensure that the process includes a duty of care to ensure that all employees are aware of the ISP and understand how the policy may affect them. Anderson Consulting (1999) suggests that *Human Resources* will be involved in the development process to ensure that adequate communication channels throughout the organisation are formed to communicate the ISP and to ensure that employees can "comment" on the policies if necessary. Also, issues such as changes to job descriptions, motivation, training and policy enforcement, or policing, will be important roles for *Human Resource* representatives to be involved with throughout the lifecycle of the ISP.

Executive Management

As with any initiative at the strategic level it is important to involve senior management in that initiative for it to succeed. In particular, in ISP development the involvement of senior management is a key success factor in the development and implementation of policy (Kadam 2007). Woodward (2000) states that the impetus for ISP must come from senior management. This is also echoed by many other researchers who state that corporate management must be involved in policy development (Baskerville 1988; Leinfuss 1996; Robinson 1997; Szuba 1998; Tudor 2001). This is further emphasized in terms of the success of development: *"Successful implementation of a meaningful information security program rests with the support of top management"* (State of Oregon 1998).

Business Unit Representatives

At the business unit level of an organisation the ownership of systems and information are often defined. Tutor (2001) states that the resource owner needs to be involved in ISP development as they best understand the resources being protected. Swanson (1998) concurs, stating that information owners must be involved in the development as they are responsible for ensuring that security for their information is effective. In many cases though, the owner of the information or the system is simply assumed to be involved with policy development (Baskerville 1988).

In addition to information owners, other business unit managers may also be involved in policy development. Warman (1992) found that junior managers, with responsibility for functional areas were significantly involved with policy development as they were required to support implementation and usage of the developed policy. Anderson Consulting (1999) also suggests that managers at the business unit level must be involved with policy development to ensure successful implementation, use and ongoing functionality of the policy within organisations.

Public Relations

An interesting stakeholder role that organisations are beginning to involve in the ISP development process is the *Public Relations* group within the organisation (Anderson Consulting 1999). As security becomes more of an issue for an organisation the Public Relations stakeholders need to show the public that the organisation is committed to security. This is extremely important if the organisation has a security incident. It is expected that this stakeholder role will only be present within large organisations.

External Representatives

In many cases for organisations it may be necessary on occasion to involve other people not mentioned previously. For instance, for some organisations it may be necessary to involve customers, suppliers and other external entities. Baskerville (1988) suggests that outside clients who are dependent on organisations systems should be involved in ISP development. Also, where there are strong strategic links between organisations the second organisation may need to be consulted in ISP development. For instance a major retailer might develop a policy which may impact all their suppliers who are directly linked to the retailer‘s computer systems for order procurement, warehousing and distribution. Failure to consult with their suppliers may cause problems in ongoing strategic relationships between the organisations (Bowersox et al. 2002).Summary of Stakeholders and Expert Interview Outcomes

As previously mentioned, in the contextual interviews, interviewees were asked two main open ended questions: “How are ISPs developed in your organisation, including who is involved with the development?” and “Which stakeholders should be involved with the development, implementation and evaluation of security policies?”. In answering the first question, all experts identified a number of stakeholders as having a stake in development. Subsequently, later in the interviews when experts were asked the second main question, a similar group of stakeholders were identified, as shown in Table 3, which were similar to those previously identified from the first question. Stakeholder roles as we have used them are shown in brackets in Table 3.

Table 3: Contextual Interview Identified Stakeholders

Expert	**Identified Stakeholders**
Fred	Business Representatives (*Business Unit Representatives*) Human Resources (*Human Resources*) IT Staff (*ICT Specialists*) Legal Representatives (*Legal and Regulatory*) Security Manager (*Security Specialists*) Senior Management (*Executive Management*)
Greg	Chief Technical Officer (*Executive-Management*) Corporate public affairs (*Public Relations*) Human Resources (*Human Resources*) Legal services group (*Legal and Regulatory*) Privacy officer (*ICT Specialist* – job to ensure IT was aligned with privacy legislation) Representative sample of users (*User Community*) Security Manager (*Security Specialists*) Senior Business stakeholders (*Business Unit Representatives*) Senior executive (*Executive Management*) Some operations level staff across several areas (*User Community*)
Hilda	Application business owners (*Business Unit Representatives*) External consultants (*External Representatives*) Internal control - legal, public relations (*Public Relations*, *Legal and Regulatory*) Personnel Department (*Human Resources*) Security and Network Specialist (*Security Specialists*) Systems / IT Management (*ICT Specialist*) Users (*User Community*)
Inga	IT specialists (*ICT Specialist*) Security Manager (*Security Specialists*) Business unit heads (*Business Unit Representatives*) Senior Executive (*Executive Management*) Human Resources (*Human Resources*) External Auditor (*External Representatives*)

Table 4 shows which stakeholder roles identified in the literature are also identified by experts as important to consult in the development and quality assessment of the ISP. As can been seen in Table 4, the *ICT Specialist*, *Security Specialist*, *Business Unit Representative*, *Human Resource* and *Executive Management* roles were identified by all of the security experts as being required to be involved in the development and quality assessment process. *Fred* states that senior management must be consulted *“so they understand what we are trying to do, not only in IT, but in other areas corporate wide”*. This is in general agreement with the other experts.

Table 4: Identified Stakeholder Roles by Expert

Stakeholder Role	*Fred*	*Greg*	*Hilda*	*Inga*
Business Unit Representatives	•	•	•	•
Executive Management	•	•	•	•
Human Resources	•	•	•	•
ICT Specialists	•	•	•	•
Security Specialists	•	•	•	•
Legal & Regulatory	•	•	•	
Public Relations	•	•	•	
User Community		•	•	
External Representatives			•	•

Two of the stakeholders were not identified by one of the experts: *Legal and Regulatory* and *Public Relations*. This may be because *Inga*'s organisation did not have these areas involved with the process, possibly due to the "newness" of having a policy within the organisation as their policies were only 11 months old.

The *External Representatives* and *User Community* were only identified by two experts each. In the case of the *User Community*, *Inga* is of the opinion that they, in large, shouldn't have a say in the policy; *"no input from users is requested. Not every employee gets a chance to say if they do or don't agree [with policy]"*. *Fred* stated that users are not consulted, and communication and enforcement of the policy is left for line managers to indoctrinate their employees. *External Representatives* were identified by two experts (*Hilda*: External Consultant, *Inga*: External Auditor). The other two experts did not see the need to have this in their current area of responsibility.

DISCUSSION AND CONCLUSIONS

The contextual interviews did not identify any additional stakeholders over those described in the literature. One major finding of this research was the recognition of the importance of the *External Representative, Public Relations* and *Human Resources* stakeholders by the expert interviewees. These three stakeholder groups were under represented in the literature and this research strengthened their inclusion in the research model. Furthermore, the experts identified that the *External Representative* stakeholder, as expected, was used in differing ways as it is aimed at the external interface to the ISP and may include auditors and consultants used for various aspects around security. Additionally, there was no evidence indicating that any of the identified stakeholder roles should be removed.

It is clear that in medium to large organisations all nine of these stakeholder roles are likely to be present, being represented by one or more individuals, who would be involved in the ISP lifecycle within the organisation. However, in smaller organisations due to the size of the organisation, individuals would be more likely to be involved in more than one stakeholder role and some stakeholder roles may be outsourced. To adequately develop an ISP as many roles as possible should be included in the development process. This will provide a comprehensive perspective of all stakeholders on the development of the ISP.

This research has identified and has confirmed with practitioners the stakeholder roles that should be included in an ISP development lifecycle. As such organisations have a clear understanding of just who should be involved in ISP development, which allows them to ensure that a range of stakeholders are available help to define ISP. One of the benefits of the inclusion of multiple stakeholders in the policy development process is that these stakeholders become advocates for the policy. This should result in ISP's that are more acceptable to workers in the organisation, especially as a sense of ownership is given by including the variety of stakeholder as specified in this paper in the development.

What this research does not yet do is to specify how and where these stakeholders are involved in policy development. Future work will use case studies to help to understand what involvement each of the stakeholder roles has in ISP development and to determine at what stages of development this involvement will take place.

REFERENCES

Abrams, M.D. & Bailey, D., 1995. Abstraction and Refinement of Layered Security Policy. In M. D. Abrams, S. Jajodia, & H. J. Podell, eds. Information Security an Integrated Collection of Essays. Los Alamitos, California: IEEE Computer Society Press, pp. 126-136.

Abrams, M.D. & Podell, H.J., 1995. Supporting Policies and Functions. In M. D. Abrams, S. Jajodia, & H. J. Podell, eds. Information Security an Integrated Collection of Essays. Los Alamitos, California: IEEE Computer Society Press, pp. 318-329.

Anderson Consulting, 1999. Policy Framework for Interpreting Risk in eCommerce Security. , 2002(September). Available at: https://www.cerias.purdue.edu/techreports-ssl/public/pfires/.

Baskerville, R., 1988. Designing Information Systems Security, Chichester: J. Wiley.

Bowersox, D.J., Closs, D.J. & Cooper, M.B., 2002. Supply Chain: Logistics Management, New York, NY: McGraw Hill/Irwin.

Dhillon, G., 2007. Principles of Information Systems Security : text and cases., Hoboken, NJ, USA: John Wiley & Sons.

Dhillon, G. & Torkzadeh, T., 2001. Value Focused Assessment of Information System Security In Organizations. In 22nd International Conference on Information Systems.

Diver, S., 2007. Information Security Policy: A Development Guide for Large and Small Companies. , pp.1-37.

Doherty, N.F., Anastasajis, 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), pp.449–457. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0268401209000735 [Accessed June 23, 2011].

Gritzalis, D., 1997. A Baseline Security Policy for Distributed Healthcare Information Systems. Computers and Security, 16(8), pp.709-719.

Henderson, S., 1996. The Information Systems Security Policy Statement. EDPACS - EDP Audit, Control and Security Newsletter, 23(12), pp.9-15.

Holtzblatt, K., Wendell, J.B. & Wood, S., 2005. Rapid Contextual Design: A How-to Guide to Key Techniques for User-Centered Design, San Francisco, Ca, USA: Elsevier Inc.

Hone, K. & Eloff, J.H.P., 2002. What Makes an Effective Information Security Policy. Network Security, (6), pp.14-16.

Hu, Q., Hart, P. & Cooke, D., 2007. The Role of External and Internal Influences on Information Systems Security - A Neo-institutional perspective. Journal of Strategic Information Systems, 16, pp.153-172.

Kadam, A.W., 2007. Information Security Policy Development and Implementation. Information Security Journal: A Global Perspective, 16(5), pp.246-256.

Leinfuss, E., 1996. Policy over Policing. InfoWorld, 18(34), p.55.

Robinson, T., 1997. Business at Risk. Software Magazine, 17(10), pp.88-91.

State of Oregon, 1998. Guideline for Developing an Agency Information Systems Security Policy. , 20 Feb 199. Available at: http://www.state.or.us/IRMD/guidelin/secpol.htm.

Swanson, M., 1998. A Guide for Developing Security Plans for Unclassified Systems, Federal Computer Security Program Managers Forum Working Group.

Szuba, T., 1998. Safeguarding your Technology: Practical Guidelines for Electronic Education Information Security.

Tudor, J.K., 2001. Security Policies, Standards, and Procedures. In Information Security Architecture: an integrated approach to security in the organization. Florida, USA: CRC Press LLC, pp. 79-99.

Warman, A.R., 1992. Organisational Computer Security Policies: The Reality. European Journal of Information Systems, 1(5), pp.305-310.

Woodward, D., 2000. Security Policy Management in the Internet Age. , 2000(27 September). Available at: http://www.itsecurity.com/papers/wickpol.htm.