

## *Security Policy Quality: A Multiple Constituency Perspective*

**S.B. Maynard**

Department of Information Systems, University of Melbourne, Australia  
seanbm@unimelb.edu.au

**A.B. Ruighaver**

Department of Information Systems, University of Melbourne, Australia  
anthonie@unimelb.edu.au

### **Abstract.**

Although organizations are taking security policy more seriously and are beginning to adopt a lifecycle approach to security policy development, how to assess the quality of security policy is still an unaddressed issue. This paper describes the results of two case studies focusing on a multiple constituency perspective of security quality assessment in organizations. Multiple constituency theory states that multiple stakeholders should be involved in any assessment of effectiveness. The main conclusion is that quality assessment needs to be carefully managed to ensure that you have a balanced approach and to ensure that stakeholders have adequate skills and training to assess quality.

**Keywords:** *Information Security, Security Policy, Security Policy Quality, Security Policy Assessment*

### **Introduction**

With information security risks on the increase, many organizations are taking the development of strategic security policy more seriously. Rather than traditional ad-hoc security policy development, organizations are beginning to use security policy lifecycles. Whilst these lifecycles allow good management of the process of security policy development, few, if any, provide for the formal assessment of security policy. Subsequently, there is a need for organizational information security research to provide better guidance to organizations on the assessment of security policy quality.

In terms of security policy quality assessment, it seems logical that the perspectives of each of the stakeholders, or stakeholder groups, should be considered so that the views of each of the groups are taken into account. Unfortunately, in many organizations, the only assessment of security policy quality is carried out by the person who developed the policy (assuming they are still employed there), or by those that subsequently were given responsibility for policy development. Multiple constituency theory argues that the quality assessment of an artifact important to the organization should be conducted using the perspectives of multiple stakeholders (Connolly et al 1980, Cameron 1980, Pennings and Goodman 1997).

This paper describes the results of two in depth case studies that look at the stakeholder involvement in quality assessment, and how stakeholders identify and use the quality attributes and characteristics identified in the security policy quality framework proposed by Maynard and Ruighaver (2006) (see Figure 1).

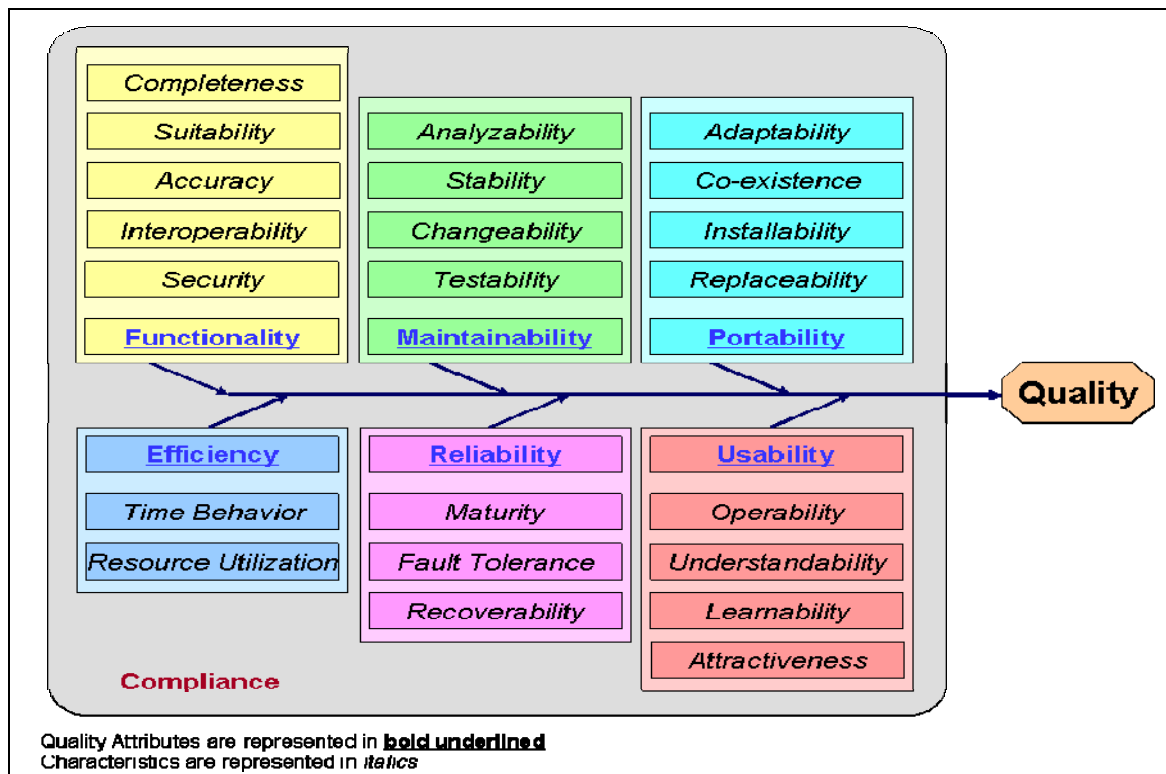


Figure 1 – The Security Policy Quality Framework

In the next section the stakeholders involved in policy development are identified. The paper then describes the two case studies and uses these case studies to identify how each of the stakeholders applies these quality attributes and characteristics to the assessment of security policy quality.

### Multiple Constituency Security Policy Quality

This research investigates the quality of strategic security policy. Hence, stakeholders identified in this section are not necessarily the relevant stakeholders for operational or acceptable use policies. Of particular interest in this study is what different stakeholder's perspectives are of security policy quality, and the involvement of these stakeholders in the quality process.

A constituent, or stakeholder, is defined as those individuals or groups that have an interest in the decisions or actions of a particular organization (Connolly et al. 1980). Connolly et al. propose the multiple constituency approach to evaluation to improve the assessment of effectiveness in organizations. From the perspective of security policy quality assessment, there are many stakeholders who should be involved with the development of security policy (Warman 1992, Abrams 1995, Henderson 1996, Leinfuss 1996, Gritzalis 1997, Robinson 1997, Swanson 1998, Szuba 1998, Baskerville 1988, Anderson Consulting 2000, Woodward 2000, Dhillon and Torkzadeh 2001, Tudor 2001). Unfortunately, in these research papers no consistency can be found on the terms used to describe the various types of people involved, with many overlapping terms used.

The stakeholder groups, as we have defined and named them based on the above research are the:

- ICT Specialists Those stakeholders whose primary responsibility is in the ICT field.
- Security Specialists Those stakeholders whose primary responsibility is in the Security field.
- Executive Management Those stakeholders who are at high level of the organisation, with strategic responsibilities.
- Business Unit Representatives Those stakeholders who are in management positions within the company that represent their particular field.
- User Community Those stakeholders whose primary responsibility is in the use of the strategic security policy to implement other policies within the organisation.
- Human Resources Those stakeholders whose primary responsibility is human resource management within the organisation.
- External Representatives Those stakeholders who are indirectly impacted by the strategic security policy. These may be the traditional “Users” of ICT in an organisation.
- Legal & Regulatory Those stakeholders who have governance responsibilities and who are focusing on policy from a legal or regulatory perspective.

### **Case Study Organizations**

The research described in this paper is informed by two in depth case studies conducted in medium sized organizations in Australia. In both organizations, data was collected through interviews, email discussions and from organizational documentation, including security policies.

The first organization (*RetailOrganization*) is a privately owned retail organization that operates on a franchisee basis. It has about 200 employees in its offices and has a turnover of over 800 million Australian dollars. The research focus within this case study was on the main business, excluding the franchised stores. A total of 6 people were interviewed in *RetailOrganization*. These interviewees represented six out of the eight constituent group identified above, excluding the External Representative and Legal and Regulatory stakeholder groups.

The security policy in *RetailOrganization* was developed in May 2000 in a response to the need of having policies in place to handle employees having access to the internet, which was about to be released to the organization at large. The culture of the organization about security is relaxed. Employees know about security and what they are meant to and meant not to do, but there are frequent minor incidents. From a managerial perspective security has some importance, although the security policies are not being enforced. A new CEO for the organization was hired in late 2004 and there was a shift in the perceptions of security and in the security policy, but the culture as at the time of the case study had not changed enough in the organization for employees to recognize that security was paramount to the organization. At the time of this case study (2005), case study personnel within the IT department were beginning to focus on the redevelopment of security policy.

The second organization (*ITOrganization*) is a publicly owned IT services organization that has offices in eight countries. The organization has annual revenue of 80 million Australian dollars a year and employs over 220 staff globally. A total of 12 people were interviewed within this organization. These interviewees represented all of the stakeholder groups we identified above.

The security culture within *ITOrganization* was a total opposite of *RetailOrganization*. Employees were immensely aware of security, and of the security policies in the organization. In terms of security policy the organization had recently revisited the security policy development lifecycle and had developed a new security policy which has just been implemented. This policy was designed to actively encourage all employees' participation in security, and superseded the outdated and rarely consulted security policies developed 8 years earlier.


Other than for policy document revisions, there was no evidence of formalized quality assessment of security policy in either case study. Only in *ITOrganization* was there evidence that any quality assessment was conducted, although, the assessment of quality was a side effect of the training process implemented where employees were encouraged to comment on the policies as they were trained.

### **Case Study Results**

In each of the interviews conducted, stakeholders were asked about how they were involved with the security policy lifecycle, in particular with assessing the quality of policy. This gave participants a chance to describe the attributes and characteristics that they use in assessing security policy quality and allowed us to gauge their interest in each of the characteristics without influence by the researchers. Once participants discussed quality in their terms, they were then asked more specific questions, based on the framework, about each of the quality attributes and characteristics. This allowed us to gauge their interest as well as their knowledge and skills related to these attributes and characteristics.

Before the stakeholder's perspectives on quality attributes and characteristics are discussed in more detail, a general overview of our findings will be presented. Table 1 shows the level of interest that stakeholders showed in each of the characteristics. A high level of interest indicates that the characteristic was initially identified by the stakeholder group and was thought to be important. A low level of interest indicates that the characteristic did not come up in the interview until the researcher asked specific questions resulting in the expression of some, but not high interest, by the stakeholder. Medium interest indicates that the researcher initially discussed the characteristic and the stakeholder group had high interest, or that individual stakeholders identified the characteristic, but there was some discordance within the stakeholder group as to its importance. No interest, indicates that when discussed the stakeholder group did not think the characteristic was important to them at all.

		Count	Executive Management	Business Unit Representatives	User Community	Human Resources	ICT Specialists	External Representatives	Legal & Regulatory Department	Security Specialists
			Stakeholders							
<b>Compliance</b>		7	H	H		H	H		H	H
<b>Functionality</b>										
Completeness	7	H	H				H			H
Suitability	8	H	H				H	H	H	
Accuracy	6		H				H			H
Interoperability	6									
Security	5	H	H							
<b>Maintainability</b>										
Analyzability	1									
Stability	0									
Changeability	7		H							
Testability	5									
<b>Portability</b>										
Adaptability	6									
Co-Existence	6							H		
Installability	6									
Replaceability	2									
<b>Efficiency</b>										
Time Behaviour	4									H
Resource Utilization	5									H
<b>Reliability</b>										
Maturity	3									
Fault Tolerance	1									
Recoverability	0									
<b>Usability</b>										
Operability	8	H						H		
Understandability	8	H	H	H	H	H	H			H
Learnability	7	H	H	H		H	H			H
Attractiveness	0									



High Med Low None  
Level Of Interest

Table 1 : A Multiple Stakeholder Perspective of the Security Policy Quality Framework

Table 1 illustrates that there is no interest shown by constituent groups in assessing the attractiveness, recoverability and stability characteristics. As explained later in the paper, this was not unexpected. In contrast, constituent groups tended to show high interest in the characteristics understandability, learnability, suitability and compliance. Of further interest, the Executive Management, ICT Specialist, Security Specialist and Business Unit Representative stakeholder groups identified the most characteristics in which they would be interested in assessing during the quality assessment. Again, this was not unexpected.

This section will now look at each of the high level attributes discussing the attribute's characteristics in terms of the case studies briefly described earlier, identifying which

stakeholders were involved in assessing quality and how they defined quality. Unfortunately, due to the limitations on paper size, it is not possible to discuss each and every characteristic in depth within each attribute. As such only those characteristics which present interesting challenges will be discussed in depth.

### **A summary of quality attributes**

This section presents a summary of the findings in the case study with regard to the multiple constituency approach to security policy quality assessment.

#### ***Functionality***

The first attribute of the quality model as developed by Maynard and Ruighaver (2006) is *functionality* which in essence is the utility of the security policy; whether it is thought to be useful to the organization in terms of *completeness*, *suitability*, *accuracy*, *interoperability* and *security*. *Functionality*, along with *usability*, received the highest level of interest from stakeholders. All stakeholder groups identified two or more of the *functionality* characteristics as important. Of these characteristics *security* was the least identified, whereas *suitability* was identified by all the stakeholder groups.

In security policy quality assessment, *completeness* would be expected to be important to stakeholders in assessing security policy and was in fact identified by all the stakeholder groups, except for *Human Resources*. To adequately assess whether the security policy is complete from a quality perspective a number of skills are required. To enable consideration of the breadth of the policy, an in depth knowledge of the organization as a whole is required, as is knowledge about the risks that the organization has and wants to mitigate, which leads to knowledge about security in order to mitigate these risks. Furthermore, knowledge about the implementation and ongoing use of the policy is required. Whilst there are seven constituent groups interested in *completeness*, some of these groups have limited skills in these areas, and some groups have limited interest in the *completeness* characteristic. For instance, it is clear from the case studies that the *External Representative* stakeholder group did not have these skills.

Whilst the *suitability* characteristic should be fairly simple to assess there are two aspects that must be considered. *Suitability* can be thought of as whether or not the security policy supports the organisation in achieving its goals. It can also be whether or not the security policy addresses the risks that have been deemed important to mitigate. As such, its assessment should be conducted by those stakeholder groups that possess a thorough understanding of how the organization functions from a business process perspective, along with those who know the risks that the organization faces and what policies are in place to mitigate those risks. *Suitability*, as shown in Table 1, was one of the three characteristics that all stakeholder groups had an interest in within the quality assessment. Interestingly though, within *Retail Organization*, only four out of the eight stakeholder groups expressed interest in this characteristic. This difference could be attributed to the focus of the organizations. As Executive2\_1 states as part of the development process within *IT Organization*, they needed to “get an understanding as to what would work and what wouldn’t” from people within the organization. Whereas, in *Retail Organization* it was not apparent if this type of higher level discussion ever took place.

The assessment of *accuracy* should focus on whether or not the security policy is performing in a manner in which it is intended by the organization. *Accuracy* was defined in a similar manner across the stakeholders in the case studies, and in essence

could be summarized as whether the policy performs as it should as defined by the organisation. This means that even if an organization has a policy for less than ideal reasons, such as for the sake of having a policy to meet compliance of legislation, that it can be assessed on these terms. Whilst *accuracy* is of interest to six of the eight constituent groups, within *RetailOrganization* only the *ICT Specialist* and *Security Specialist* stakeholder groups were interested.

The assessment of how a policy interacts with other policies within an organization is an area that, whilst important for clear understanding of policies, may not be consistently assessed by organizations. At worst, contradictory policies may be produced, with organization personnel being unsure where they stand. *Interoperability* could be complex to assess, and a thorough understanding of the organizational policies is required. As such it is likely that higher levels of the management structure, where there is cross departmental concerns, may be more interested in it rather than it being based in the security or ICT domain. Consequently we expected the *Executive Management*, *Business Unit* and *Legal and Regulatory* stakeholder groups to be involved in assessing the *interoperability* of the security policy with the other policies of the organization. Surprisingly, *interoperability* was considered by six out of the eight constituent groups studied, which is more than we expected, but only the *Executive Management* stakeholder group showed real interest within both case organizations.

The *security* of security policy is defined as whether or not there is information in the security policy that could be detrimental to the security of the organisation if it was released in the public domain. This characteristic tended to be discussed by stakeholders in terms such as, “they are fairly generic so I don’t think it is much of an issue if they were to get out” (Manager2\_1). But then, to gain access to the policies in each of the case sites, permission was needed from the CIO or CEO of the organization. In both of the organizations, as stated above, whilst there was interest in *security*, only the *ICT specialist* stakeholder group in *ITOrganization* considered *security* of policy when policy quality was previously assessed. However, there was good interest in the concept of securing, or ensuring the appropriateness of the contents of the policy with four additional stakeholder groups expressing interest when this attribute was discussed by the researchers. To adequately assess this characteristic, knowledge about security and appropriateness of security policy statements with regard to the organization is required, so the additional interest by other stakeholders, except for the *Security Specialists* was unexpected.

### ***Maintainability***

Whilst, one would think that policy *maintainability* is important in assessing the continuity of the policy development lifecycle during the quality assessment process, Table 1 shows that there was little interest in several of the characteristics of *maintainability*. Although there is indication that some of the *maintainability* characteristics are important in assessing quality, it is not clear as to the reasons why stakeholder groups do not see the import of these characteristics. We believe that the concept of *maintainability* is one of the three areas of the quality model that is directly influenced by the sophistication (or maturity) of the organizations security policy development process.

There was little interest by stakeholder groups in the concept of *analyzability*. Only in *ITOrganization*, was any interest at all shown in this characteristic, and only by the *ICT Specialist* stakeholder group. This stakeholder was interested primarily in

understanding the deficiencies in the security policy, especially when changes to the environment occurred and used this as an enabler for further policy development. The lack of interest by other stakeholder groups is somewhat concerning, as one would think that being able to determine how the policy could be improved after a breach has occurred, especially if the breach was caused by a deficiency of the policy, would be important to an organization. From the perspective of the quality framework, the issue of *analyzability* may become more important as organizations continue to revisit the policy development lifecycle and the concept of maintaining the security policy becomes more of a pressing concern. Once this occurs, the stakeholder groups specifically involved with the operate stage of the policy lifecycle, who are also involved with risk and security will need to consider *analyzability* when they are assessing policy quality.

*Stability* is one of the three characteristics of quality where none of the stakeholder groups showed interest from a quality assessment perspective. Whilst in some ways this is understandable, the concept of building a policy that should not overly change over time is still an important. One possible explanation for this is that in each of the case organizations, security policies were only on their first or second iteration through the policy development lifecycle. This lack of maturity within the policy may be a factor that will influence the importance of *stability* to stakeholder groups.

*Changeability* as defined by the stakeholders is the ability for the policy to change in response to environmental or technological changes. *Changeability* is the only one of the characteristics of *maintainability* that had a large amount of interest from stakeholder groups across both organizations. However, the interest from stakeholder groups is inconsistent between the two case organizations, with only the *User* and *Executive Management* group interested in *changeability* in both organizations.

It is surprising that *changeability* is not more popular as it is one of the characteristics that one would think of as an obvious issue in security policy, both from a theory and practical perspective and one that is fairly easy to assess. *Changeability* is interesting, as on one hand, the security policy must be able to change in accordance with changes to technology, to the organization and to the external environment, but on the other hand, the *stability* of the policy is necessary. A balance between *changeability* and *stability* is the probable solution and stakeholder groups need to consider this upon assessing quality from these perspectives. Because of this interdependence on *stability*, one would expect that the stakeholder groups that assess *changeability* should also have a focus on *stability* to ensure this balance is achieved.

The concept of *testability* in security policy terms seems to be alien to many stakeholder groups. In the case study organizations, the security policy was implemented essentially through pushing it through the organization on a certain date, and then training all personnel. In the training, issues that people had with the policy were then addressed. There was no formalized testing akin to that done in software development, although there was some interest in *testability* of security policy within *ITOrganization*, as shown in Table 1. In fact, when it was suggested that *testability* could be accomplished by a staged implementation of security policy within the organization, each of the interested stakeholder groups within *ITOrganization* thought that this could be worth while; however in *RetailOrganization* this was not observed.

### ***Portability***



For *RetailOrganization*, *portability* was not an important concept for the assessment of information security policy quality, mainly because of their business structure and the fact that they are wholly operating within Australia. However for *ITOrganization*, because of their international nature, concepts of *portability* were considered to be more important in assessing the quality of their security policy. As a result, no stakeholder groups from *RetailOrganization* identified any of the characteristics of *portability* when discussing quality, and even when specifically pushed for these characteristics there was no interest in them. Contrastingly, in *ITOrganization* there was good interest from many of the stakeholder groups, with evidence that most *portability* characteristics were assessed when assessing quality.

In *ITOrganization* a major concern of some stakeholders was whether or not they can cater to the local environment when installing policies in overseas offices, and if not, whether the policy could be adapted to do so. The key to *adaptability* according to *ITOrganization* is to ensure that policies are written in such a manner that they can be modified to suit overseas conditions, without altering the meaning behind the policies. “there would be some issues in any country in which we operate and we would need to comply with the applicable policies ... it is the usual practice to have this checked for adequacy” (Executive 2\_3). The most appropriate stakeholder groups for assessing the *adaptability* of the security policy would need skills and knowledge about the differing requirements of the organization, and may have had to implement, or use the policy in differing environments. In addition, a security perspective would be required to ensure that changes made to the security policy did not compromise the policy.

*Co-existence* of the security policy deals with whether or not the security policy can exist in parallel with other organizational policies. This characteristic was important to four of the eight stakeholder groups within *ITOrganization*, who essentially define *co-existence* as whether or not the security policy is complemented by other policies within the organisation. The issue here is about the differences between organizational policies where you are rewarded for doing things, and the security policy where often you are being told what not to do. The enabling nature of other organizational policies may cause conflicts with the security policy because on one hand you are being told to be goal oriented – being judged on how well you do something, versus being told no you can’t do that, it breaks security.

The *installability* characteristic was utilized by six stakeholder groups in *ITOrganization* whilst assessing quality. In assessing the *installability* it is important that local knowledge of the environment is available as well as knowledge about the impact of any addendums to the security policy. As such it would be expected that the *Business Unit Representative* and *Security Specialist* stakeholder groups would have interest in this characteristic. This was found in the case studies, but the additional stakeholder groups, particularly the interest from the *Executive Management* stakeholders was surprising as the installability is not really a senior management concern.

Of the four *portability* characteristics *replaceability* is the least thought of in assessing quality by the stakeholder groups. Only the *Business Unit Representative* stakeholder group indicated that the policy may replace other policies and as such, *replaceability* may need to be assessed in the quality process. Whilst the low interest was unexpected, these findings are indicative of the nature of security policy development in many organizations where security policies are usually developed by the ICT area, are

implemented, and then only have precursory attention after that, until they are revisited. Unfortunately, this revision generally takes the form of a redesign, often from scratch. This then replaces the policy which is often way out of date.

### ***Efficiency***

*Efficiency* is the second of the three quality attributes that depends on the maturity of the security policy development process. As the sophistication of the development process increases, stakeholders will be more likely to consider the *efficiency* of all facets of security policy development. Issues such as the selection and wording of the security policy statements may become important as particular resources or time constraints may occur. In the case studies, significant interest was shown in the *efficiency* attribute by *ITOrganization*, whilst in *RetailOrganization* only the *Security Specialist* stakeholder was interested in the efficiency characteristics.

Initially, it was thought that there would be little evidence that organizations would consider *time behavior* in their development of security policy. As such, it was surprising the amount of interest stakeholders exhibited towards *time behavior* in the case studies, with four stakeholder groups, including three within *ITOrganization* and one in both organizations having some focus on the *time behavior* characteristic. What is clear from both case studies is that the security policy development in both organizations does not yet take into account the wording of the policy in terms of time efficiency, and policy statements do not seem to be compared against similar statements to try and select the best, not only from an *efficiency* perspective, but also with *usability* in mind. If organizations get to this stage of sophistication it will be important that whilst attempting to maximize *time behavior*, the integrity of the policy and its *usability* must also be maintained.

The amount of resources required to implement, enforce, maintain and use the policy is described using the *resource utilization* characteristic of *efficiency*. Issues such as duplication of tasks (which is important to ensure that the policy is fault tolerant), and how the policy is enforced are considered in this characteristic's area. In the case study organizations, there is limited interest in *resource utilization* in the assessment of security policy quality. In *ITOrganization* there are five stakeholder groups who consider resource utilization to some degree, with one additional interested stakeholder group being identified in both case studies. The difference between *ITOrganization* and *RetailOrganization* could be attributed to the fact that *RetailOrganization* essentially pushes the policy out to the organization without much involvement of other stakeholders, whereas in *ITOrganization* good involvement and awareness of policy is apparent.

### ***Reliability***

The final attribute that depends greatly on the sophistication of the security policy development lifecycle is *reliability*. Unsurprisingly, due to the low sophistication of security policy development within the case organizations, this attribute has the least amount of interest from any of the stakeholder groups. This may also be attributed to a lack of understanding from stakeholder groups as to how *reliability* is important in security policy. Stakeholder groups that are expected to be involved in *reliability* quality assessment should be trained in the concepts of *maturity*, *fault tolerance* and *recoverability* for the importance of *reliability* in security policy assessment to be realized.

*Maturity* was the most discussed characteristic of *reliability*, with interest shown by three stakeholder groups, one in *ITOrganization*, one in *RetailOrganization* and one in both organizations. *Maturity* of security policy within an organization may be indicated by the number of changes to the policy in the last cycles through the lifecycle, or by a decrease in the number of changes made to the policy as a result of incidents. When stakeholder groups assess the *maturity* of security policy, the factors mentioned previously may give indications that the policy lifecycle is mature, and as such it is therefore likely that the policy itself is of high quality from this perspective. As a result, those who are undertaking the quality assessment from this perspective must be aware of how the policy lifecycle operates, and should be involved in the enforcement and incident containment areas.

As expected, *fault tolerance* has a poor representation of stakeholder groups identifying it as an important area to assess when looking at the quality of security policy. The focus of *fault tolerance* is on ensuring that there is redundancy within the security policy. This may include ensuring that responsibilities are clearly stated in the policy and that there is a fall back in case personnel are sick or leave the organization. One would expect that stakeholder groups involved with assessing *fault tolerance* would have knowledge about the security policy and how it has been developed and would understand how the policy statements are implemented in the organization. We would expect that based on this the *ICT Specialist* and *Security Specialist* stakeholders should be involved, however only the *ICT Specialist* stakeholder group within *ITOrganization* showed any interest.

*Recoverability*, deals with returning something to a normal state. In terms of security policy quality there is no evidence in the case studies that supports the concept of *recovery*. Certainly, however aspects that are related to *recoverability*, such as the ability for organization to change the security policy to prevent further incidents, are covered elsewhere within in the framework; in this example this would be covered in *changeability*.

### ***Usability***

Within the *usability* attribute of quality, three of the four characteristics received high levels of support for including them in the quality assessment process. What is interesting is that when many of the stakeholder groups initially discussed the idea of quality from the *usability* perspective they represented it as “*understandability*”. However, as the concepts were further discussed it became apparent that they were also looking at several other characteristics of *usability*, in addition to *understandability*. So when many of the stakeholders discussed “*understandability*”, they tended to talk about being able to read the policy, learn what is in it, and then put it into practice, which equate to the characteristics of *usability*: *understandability*, *learnability* and *operability* respectively. In terms of the process of *usability*, one must understand the security policy before it can be learnt. Once it is learnt then it is possible to operationalize it in day to day activities. The first three characteristics *understandability*, *learnability* and *operability* explain this concept.

*Understandability* is the ease of comprehensibility of the policy. Unsurprisingly, there was interest from all stakeholder groups identified in the cases in the *understandability* of the security policy when assessing quality. Given that all stakeholders have identified this area as important in assessing quality, it is clear that a compromise might

be made for time and cost reasons as to which stakeholders should actually be assessing *understandability*.

The ability to learn the requirements of the security policy so that it can be made operational was considered an important characteristic in quality assessment by all stakeholder groups except for the *Legal and Regulatory* stakeholders. Within each of the organizations an approach taken to help stakeholders with *learnability* is to remind them of policy areas at regular intervals. “We pick a particular element of the policy and we say for the next fortnight, or whatever period we focus on that particular item, and we tell people that we are going to do it, giving them warning, then we start enforcing it.” (*Manager 2\_1*).

Each of the stakeholder groups, to varying degrees across the case study organizations focused on the utility of the security policy with regard to the ability of stakeholders being able to put it into practice. In *ITOrganization* all stakeholder groups perceived the *operability* characteristic as important to include in quality assessment. Within *RetailOrganization* though, only the *Executive Management, Business Unit Representatives* and *User Community* stakeholder groups were of like mind. Like *understandability*, it may not be appropriate to include all the interested stakeholders in assessing the *operability* characteristic. One would expect that the appropriate stakeholders would be a combination of technical and non technical and should include those who must implement and abide by the policies

The fourth characteristic, *attractiveness*, was not considered to be an important characteristic by any of the stakeholder groups, and we believe there may be good reasons for this. As stated earlier in this section, stakeholders tended to be more concerned with the *understandability* of the written policy document, rather than if it looked good. A dependency between *attractiveness* and *understandability* is apparent as some stakeholders may have a better understanding if the document is presented in an attractive manner. As the organizations become more intranet dependant the *attractiveness* characteristic may become more significant as importance will need to be placed on how the policy document “looks” to the stakeholders when it is distributed and available in electronic form. No evidence was found of interpretations about *attractiveness* of the policy itself, for instance whether the choice of policy statements has been influenced by personal preferences of those stakeholders involved in implementing or enforcing the policy.

### ***Compliance***

The final attribute of the quality model is *compliance*. This attribute is different from the other attributes as it plays an overarching role. As such, it is probably the most important attribute and is also the one attribute that should obviously be found within all organizations. And, indeed, all stakeholder groups except for the *External Representatives* identified *compliance* as an important attribute to consider with the quality assessment. Considering the effectiveness and cost of having so many constituents involved in assessing this characteristic of *compliance*, it might be better if some of the stakeholder groups left this area alone to concentrate on other areas of interest.

### **Conclusion**

As security policy lifecycle usage increases within organisation, and they become more proficient in policy development, organisations will need to focus on the formal

assessment of security policy quality. In this paper we presented two case studies and used these cases to study stakeholder involvement in security policy quality assessment.

It is clear from the summary of this research (Table 1) that there is an imbalance with the number of stakeholders involved with the differing quality characteristics. In a multiple constituency assessment of security policy quality it will be important that there is a balanced approach to quality assessment, to ensure the process is efficient for all involved and that the quality assessment covers each of the quality attributes in an appropriate manner. As such, one might consider that there are a number of characteristics where it is not economical to have so many stakeholder groups involved with the quality assessment, and that some stakeholder groups could focus their effort elsewhere.

Also clear from the case studies is the need to educate stakeholders on the nuances of several of the quality characteristics, particularly in the *usability* area. By clearly defining each of the characteristics, differing stakeholder groups will be able to conceptualize each characteristic in a similar manner and make informed judgments for the characteristic based on a common ground. Having a clear definition of characteristics will prevent misunderstanding of stakeholder groups as to the utility of each characteristic.

Where there is little or no interest in characteristics shown by stakeholders, further work is needed to explain the importance of these characteristics, and to provide suggestions for stakeholder involvement so that a balanced approach is achieved. While we discussed some tradeoffs between characteristics of policy, such as the trade off between *completeness* and *understandability*, we believe more research is needed in identifying other tradeoffs. We also identified some of the skills that may be required by constituent groups to adequately assess quality for the more difficult to assess characteristics.

Our current research in this area now concentrates on the development of a multiple constituency framework for the quality assessment of security policy. This will incorporate the research conducted as reported in this paper, in conjunction with research investigating the importance of each of the quality characteristics to organizations. Research is also being conducted on the incorporation of formalized security policy quality assessment within the security policy lifecycle.

## References

- Abrams, M. D. and Bailey, D. (1995). Abstraction and Refinement of Layered Security Policy. Information Security an Integrated Collection of Essays. M. D. Abrams, S. Jajodia and H. J. Podell. Los Alamitos, California, IEEE Computer Society Press: 126-136.
- Anderson Consulting (1999). Policy Framework for Interpreting Risk in eCommerce Security. 2002.
- Baskerville, R. (1988a). Designing Information Systems Security. Chichester, J. Wiley.
- Cameron, K. (1980). "Critical Questions in Assessing Organizational Effectiveness." *Organizational Dynamics*: 66-80.
- Connolly, T., Conlon, E. J. and Deutsch, S. J. (1980). "Organizational Effectiveness: A Multiple Constituency Approach." *Academy of Management Review* 5(2): pp 211-217.

- Dhillon, G. and Torkzadeh, T. (2001). Value Focused Assessment of Information System Security In Organizations. 22nd International Conference on Information Systems.
- Gritzalis, D. (1997). "A Baseline Security Policy for Distributed Healthcare Information Systems." *Computers and Security* 16(8): 709-719.
- Henderson, S. (1996). "The Information Systems Security Policy Statement." *EDPACS - EDP Audit, Control and Security Newsletter* 23(12): 9-15.
- Leinfuss, E. (1996). "Policy over Policing." *Infoworld* 18(34): 55.
- Maynard, S. and Ruighaver, A. (2006). What Makes a Good Information Security Policy: A Preliminary Framework for Evaluating Security Policy Quality. 5th Annual Security Conference, Las Vegas, Nevada USA, Information Institute.
- Pennings, J. M. and Goodman, P. S. (1977). *Toward a Workable Framework*. London, Jossey-Bass Limited.
- Robinson, T. (1997). "Business at Risk." *Software Magazine* 17(10): 88-91.
- Swanson, M. (1998a). *Guide for Developing Security Plans for Information Technology Systems*, NIST.
- Szuba, T. (1998). *Safeguarding your Technology: Practical Guidelines for Electronic Education Information Security*, Technology and Security Task Force, National Forum on Education Statistics, US Department of Education.
- Tudor, J. K. (2001). *Security Policies, Standards, and Procedures. Information Security Architecture: an integrated approach to security in the organization*. Florida, USA, CRC Press LLC: 79-99.
- Warman, A. R. (1992). "Organizational Computer Security Policies: The Reality." *European Journal of Information Systems* 1(5): 305-310.
- Woodward, D. (2000). *Security Policy Management in the Internet Age*. 2000.