Policies for Construction of Information Systems' Security Guidelines

Five approaches

MIKKO T. SIPONEN
University of Oulu, Department of Information Processing Science

Key words: Security policies, end-user guidelines

Abstract: Information security research has a bias towards formal and small-scale policies. This research tradition, albeit important, has neglected the non-formal and non-computer oriented security policies. Yet the current classifications concerning security policies do not fully address the issues in security policies within information systems. Firstly, a new classification of (two categories) security policies will be depicted. Secondly, and the main contribution of this paper, five approaches to construction of end-user guidelines will be put forth, including the strengths and weaknesses of these approaches.

1. INTRODUCTION

It is widely agreed that a "security policy" is crucial in achieving security in an organization (e.g. Glasgow & MacEwen, 1987; Straub, 1990; Warman, 1992; Wood, 1995; Summers, 1997; Straub & Welke, 1998). To increase our understanding of the research issues on security policies, we may classify security policies into two categories, namely 1) Computer-oriented or technical policies (often in the area of computer security); and 2) People-oriented/organizational or non-technical policies (mainly in the area of information system security). With regards to the first category, various computer security policies and models such as AM, DAC, MAC and RBAC have been presented in order to satisfy different information security requirements, such as confidentiality/secrecy or integrity (or both) (e.g. McLean, 1990; Foley, 1991; Sandhu, 1993; Sandhu & Samarati, 1994; Boswell, 1995; Castano et al., 1995; Summers, 1997; Sandhu, 1998). The

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

second category, the people-oriented/non-technical policies (e.g. organizational security policy) has not got equal attention compared to the first category. For some reason, the field of security has a bias towards small-grained protection of entities within computer systems, although people-oriented policies are the most crucial (Thomas & Sandhu, 1994;Warman, 1992). Due to such negligence of human processors, security research from the viewpoint of IS, is still considered to be in its adolescence (Baskerville, 1989 p. 242).

Regarding people-oriented policies, only a few studies (published in Journals and International conferences) exist, including Lindup (1995), Wood (1995; 1996b; 1996c; 1997a; 1997b) and Anderson (1996). Comparing these people-oriented/non-technical policies to computer-oriented policies, the difference in the level of maturity of the research is quite obvious. In contrast to computer-oriented policies (category one), the studies on people-oriented or non-technical policies are difficult to perceive as being the result of an application of a serious discipline, in light of any reference science (whatever that would be) or research method (excluding Anderson, 1996; Lichtenstein & Swatman, 1997; Lupu and Sloman, 1997; Yialelis et al., 1996 - of which the two latter are technical-oriented). Rather, they seem to be "justified", if they are justified at all, merely by reflecting personal experiences, opinions, preferences or feelings of the authors. Unfortunately, personal opinions or preferences have no place in science (Chalmers, 1982 p. 1). Perhaps one reason behind this lack of disciplined research is that non-technical policies (category two), due to their non-formal nature, have not gained the interest of mathematically/technically oriented mainstream security scholars. Rather, they have been left for consultants and similar practitioners, whose main interests are not scientific research. Although, it may be difficult to develop the people-oriented policies using mathematical/philosophical logic as the main reference discipline, we should not hinder attempts to apply other reference disciplines. With respect to the first category, computer-oriented policies, the research methods and reference disciplines seems to be already relevant: the "behavior" of computer systems is best modeled by logic.

This paper is based on the belief that there are non-technical policies which are relevant to the achievement of security in an organizational level, and that such policies can – and should – also be approached using methods other than mathematical modeling as a main research method, as well as other reference disciplines in addition to mathematics. Security guidelines, with respect to security policy, are chosen as examples to justify this belief. However, we submit that the aforementioned claim may be valid in areas within the second category as well, and these other issues are left for future research.

In any organization, the security relevant actions of all end-users should reflect the organizational information security policy. Even though this matter is of crucial relevance in the consideration of security as a whole on any organizational level (e.g. Hale, 1996), the end-user matters concerning security policies have not received similar concern by researchers as other computer-oriented policy issues. With regards to security guidelines, only the omission of guidelines has often been reported, yet some examples of good end-user guidelines or adequate criteria for various actions, such as passwords, have been presented by Conorich (1996), Poore (1996) and Wood (1996a), for instance. Security guidelines, or chosen approaches to good security guidelines, may be adequate in a technical sense or general sense. However, they are not explored in enough detail to be considered adequate in dynamic situations or exceptional cases, thus avoiding conflicts or inconsistencies within the guidelines in such situations. Without this type of consideration there can be conflicts within the guidelines themselves. In other words, (A) two different rules within a guideline may conflict, i.e. in certain special circumstances the keeping of one rule within an information security guideline may violate another rule in those same guidelines. Alternatively, (B) conforming to the guidelines in a special circumstance would yield negative results in terms of security; or (C) adherence to security guidelines in certain circumstances averts achieving business objectives (e.g. suddenly raised business opportunity cannot be used as it would formally violate security guidelines). Moreover, (D) a literal following of the security guideline may be in conflict with higher level security policies, say, organizational information security policy. The B type of problem (i.e. due to special circumstances, "correct" actions nevertheless lead to a security breach) has been recognized and termed as "indirect failing" by Spruit (1998). The possibility of conflicts related to guidelines is also mentioned by Sibley et al. (1993). Baskerville (1995) has also identified several conflicts (including the C type of problem) in unpredictable situations. As a result, "*the IS field needs new safeguards that are less inhibitive in situations of rapid or unpredictable change*" (Baskerville, 1995 p. 245).

This paper contributes to solving these kinds of problems (A, B, C, D) by presenting five approaches to the construction of guidelines in order to avoid such conflicts. Conceptual analysis in terms of Järvinen (1997; 2000) is used as the primary research method to obtain and justify the results.

The rest of the paper is organized as follows. In section two, five approaches for construction of security guidelines are discussed. The third section summarizes the key issues of this paper.

2. FIVE PRINCIPLES FOR CONSTRUCTION OF SECURITY GUIDELINES

Different end-users form an important component from a security point of view because many uses or abuses of a system (in terms of security) directly or indirectly involve end-users. Regarding the end-user facet, security guidelines are an object of discussion with respect to security policies. Security guidelines should reflect security requirements captured by security policies as they enforce end-user compliance to the security policy of the organization in question. In other words, security guidelines express the goals of higher level policies (e.g. organizational security policy), in a low level of abstraction. Security guidelines are mainly expressed in a natural language, as they need to be easily understandable for any end-user.

The political and constructional issue of how to approach (or what principle should be used to approach) security guidelines generally, or especially in cases where rules of a guideline may not be applicable (or may not give the best possible results), will be addressed next. To see the problem, presume that one would develop security guidelines in the clinical environment on the basis of the security policy suggested by Anderson (1996). For example, principle six states, "*all access to clinical records shall be marked on the record with the subject's name, as well as the date and time*" (Anderson, p. 36). Let's further assume that this principle presumes that it is compulsory to find out and then add the subject's real name into the system. In that case, the security guidelines of nurse-tender may include the following rule:

> "*The real names of all incoming patients must be checked and the real names must be added into the system*".

Now let us consider an imaginary case in which a witness in an upcoming trial has been the victim of an attempted murder, so that they could not testify against a powerful crime cartel. However, the murder attempt was not successful and the witness was brought to the hospital for treatment. If the nurses of the hospital comply with their security guidelines literally ("add their real name into the system") it might follow that the assassin could find the witness and, for example, change the medicine in their file resulting in the death of the witness. This tale, although it is very simplified and imaginary, hopefully illustrates the problem of security guidelines: there are cases in which literal compliance is not reasonable.

To avoid such problems, five principles behind end-user guidelines will be considered and discussed next.

The first is a standard mandatory approach often seen in the military environment. Conservative approach claims that what is not allowed by information security guidelines is strictly denied irrespective of the situation in question or consequences it may raise. In other words and order is an order, to be followed no matter what. The conservative approach, albeit it is commonly applied by the security community, seems to be impractical, at least in the sense that is rigid, inflexible (more than the other approaches) and therefore mostly likely to be inapt in a dynamic environment. For example, conservative approach is inadequate for emergent organizations in terms of Truex et al. (1999) that are common in the present era - a fact which IS security should also take into account (Baskerville, 1993). To be more precise, the more dynamic the environment and changeful the workers assignments are, the more inadequate the conservative viewpoint is likely to be. Spruit (1998) argued that the number of all possibilities with respect to non-standard actions and circumstances is simply too great to cover in security guidelines. For example, in the case of the dynamic environment, it is very difficult to formülate all-inclusive guidelines, with the result that there might be situations in which certain actions not covered by guidelines are desirable, whether in terms of the mission statement or security.

According to a liberal approach, those actions (in terms of security) which are not prohibited are acceptable, *per se*. Security guidelines are to be followed literally, but if the user is faced with an issue that is not addressed by the guidelines, it follows that some appropriate action to deal with the situation is acceptable. The liberal approach is not likely to be favored by any (information) security policies, but it may be an approach in which people may be easily caught up (especially if control concerning those guidelines is loose). This is the attitude one may find toward the law; if something is not expressly forbidden, people may presume that it is allowed. The strength of the liberal approach lies in the preference of end-users, as it is likely to be more satisfactory in the eyes of end-users than the conservative approach. For example, it is easy to use given that the security guidelines do not became as thick as a statute book. The weakness of this approach relates to its nature, as it easily leads to a state of insecurity. This is almost unavoidable, as it is very difficult to compose such a set of guidelines that would cover all the relevant issues in terms of information security. And, as the principle of liberal approach suggests, if the issues not required by guidelines are not take into account in any respect, they are acceptable, which may lead to potential risks from the security perspective.

The third form is labelled as a (modified security) prima-facie approach, and is modified from Ross (1930) and R.M. Hare (1981). The idea of prima facie was originally put forth by Ross (1930) in the area of moral philosophy. According to the modified view of prima-facie, the requirements of security guidelines should be met generally. Yet they can be formally violated inasmuch as 1) the situation involves two or more conflicting requirements (in terms of business or security), and 2) the benefits of compromising those guidelines (excluding a person's egoistic/ideological benefits) clearly outweigh the benefits of complying with the security guidelines in terms of security or business objectives. The prima-facie approach is more flexible than conservative and it may lead to better situation in terms of security or business, particularly in unordinary situations that are not covered by conservative or liberal based security guidelines. Its weaknesses include, in comparison to the conservative approach, that it may better meet the preferences of end-users (consider the outlined motivational issues). The weakness of this approach from the security viewpoint relates to exception rules, i.e. what determines or justifies the actions against guidelines or actions not covered by information security guidelines. The second condition was designed to help us in this respect and for the reasons just mentioned, although it is logically possible in some respect to formulate it by other constraints, this constraint was favoured. This condition as currently presented, however, still leaves a possibility for insecure actions done in the light of the prima facie approach. For example, the sub-principle of "benefits of compromising those guidelines (excluding a person's egoistic benefits) clearly outweighs the benefits of complying with the security guidelines" contains the weakness that, in the case of conflicting rules within the guideline, it puts the judgements on users and leaves room for subjective interpretations, as it may not be unequivocal what are "benefits", for instance.

The fourth approach is superegorative by its nature. In this case, the guidelines are interpreted as a) descriptive (non-accomplishment-oriented) or b) prescriptive (accomplishment-oriented). However, in the sense that prescriptivity is not a logical demand, the guidelines prescribe an ideal or a virtuous state-of-affair that is good or courteous for the end-user to follow (but not required). Superegorative approach differs from the others, as the actions against codes are not ultimately bad, required nor punishable. It is therefore a similar approach to that often used in superegoration of virtue ethics in the area of moral philosophy. The strengths and weaknesses of the superegorative approach are similar to those of the liberal approach, except that the superegorative approach may promote more positive attitudes towards security guidelines than the liberal approach since it accentuates the virtue of observance of information security guidelines. The ease of safe use is also easily satisfied as the guidelines are not compulsory. However, neither sanctions related to the disobeying of security guidelines for purposes of deterrence nor preventive countermeasures (e.g. see Straub & Welke, 1998) can be installed if the superegorative approach is applied.

The final approaches is called universalizability, which is modified from universality theses presented in many ethical and socio-political theories such Kantian ethics, universal prescriptivism (Hare, 1981), theory of justice (Rawls, 1972) and Jewish-Christian ethics. The idea of universalizability could be used in many ways in respect to end-user guidelines. For example, the guidelines could be, in theory, replaced altogether by the principle of universality. In that case, any action by end-users would be accepted only if it satisfies the universality principle. As a second example, which is perhaps more relevant, would be a blend of the previously mentioned prima-facie principle and the universality idea. In that case, the requirements of security guidelines should be met generally, but if considered inadequate (e.g. rules are in conflict or the actions stated in guidelines in some particular situation do not seem to produce the best/adequate results in terms of security or business) the security guidelines can be violated provided that it satisfies the principle of universality. We shall divide the universality principles into "security partial" and "impartial" principles as follows:

Impartial universality principle:

Action Y is allowed if it is allowed for any X in the same or similar situation.

Security/business objective partial universality principle:

If you were the security administrator or the manager of the organization, would you allow action Y by any trustworthy X?

In the principles above, X refers to any person/worker and Y for actions. Thus, in the case of second (security partial universality) principle the end-user deliberates if they would be the security administrator (or similar) whether they would allow the action.

The strengths of the universalizability approach rests on its viewpoint in which the end-user should think as the security administrator or the manager of the organization. It should be also rather easy to use: the security guidelines can be formulated within reasonable length and the principles of universality (partial, impartial) should not be very difficult in a general sense. The main weaknesses of this approach relates to its impartiality and lack of perception of the security administrator's viewpoint. How could end-users ultimately know how the security administrator would think? However, the main contribution of this approach is that, if users applied it, it constrains users to made decisions as they were in the shoes of the security administrator. In other words, even though no one can capture another's thoughts – the user is constrained to do their best to maintain security as security administrators.

3. CONCLUSIVE DISCUSSION AND THE FUTURE WORK

The main limit of the aforementioned analysis relates to the used research method (i.e. conceptual analysis) to obtain results. The five conceptual principles presented here were only considered with the help of reference discipline: philosophy. In the long run, the conceptual analyses alone are not an adequate research approach in order to trying to solve the problem. To obtain more practical information on situations involving humans (end-users herein) with respect to relevancy and adequacy of the five principles presented, empirical studies are also needed. However, as there are no conceptual or theoretical framework hitherto presented and then considered, a conceptual framework, such as the one presented in this study, needs to be put forth as a first step.

The role of information security policies with respect to end-user computing in the organization level was considered in focusing on an approach behind security guidelines. Five possible approaches were analyzed. From those, the approach referred to as conservative is perhaps the most often used. This is true despite the fact that it is rather unsuitable for modern companies, mainly due to its inflexible nature, as it advocates that all permitted actions are explicitly described in the guidelines. Its weakness involves situations where certain circumstances would require action that is not covered by security guidelines, and therefore such an action can not be executed, no matter what positive results it may produce.

Both the weakness and strength of the liberal approach rests on the freedom that it allows the user. This approach, albeit favoured by users due to such liberality, is problematic from the security perspective as it easily leads to insecure states.

The prima-facie approach was outlined with two principles, and was argued to be flexible especially in dynamic environments. The weakness of this approach is its abstractness. In theory it leaves so much room for personal interpretation that it may lead to an insecure state.

The superegorative approach was also introduced. It states that the obeying of information security guidelines is not compulsory. Users are encouraged to act virtuously and conform to the information security guidelines.

The universalizability approach was introduced with two possible rules. The first possible rule attempted at impartiality and the second tried to put the user in security administrators shoes.

Sanctions can be associated to four approaches (punishment cannot be associated with superegoratory one) and rewards can be used together with all approaches.

The agenda for future work includes the organization of empirical studies in order to better understand the strengths and weaknesses of the different approaches presented herein. One future research question in this respect includes how the motivation of employees really correlates with the different approaches presented.

4. REFERENCES

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

Baskerville, R., (1989), Logical Controls Specification: An approach to information system security. In H. Klein & K. Kumar (eds.) systems development for human progress. Amsterdam: North-Holland.

Baskerville, R., (1993), Information Security: Adapting to Survive. Information Systems Security. Vol. 2, no. 1, pp. 40-47.

Baskerville, R., (1995), The Second-Order Security Dilemma. in W. Orlikowski, G. Walsham, M. Jones and J. DeGross (Eds.) Information Technology and Changes in Organizational Work. London: Chapman & Hall, pp. 239-249.

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

Castano, S., Fugini, M., Martell, G., & Samarati, P., (1995), Database Security. Addison-Wesley.

Chalmers, A.F., (1982), What is this thing called science? Second edition, Open University Press.

Conorich, D. G., (1996), UNIX Passwords. Information Systems Security. Vol. 7., No. 1.

Foley, S.N., (1991), A Taxonomy for Information Flow Policies and Models. Proceedings of the 1991 IEEE Computer Security Symposium on Research in Security and Privacy.

Glasgow, J.I & MacEwen, G.H., (1987), The development of proof a formal specification for a multilevel secure system. ACM Transactions on Computer Systems. Vol. 5., issue 2. Pp. 151-184.

Hale, R., (1996), End-User Computing Security Guidelines. Information System Security. Vol. 6, No. 1.

Hare, R.M., (1981), Moral Thinking: its levels, methods and point. Oxford University Press, Oxford, UK.

Järvinen, P., (1997), The new classification of research approaches. The IFIP Pink Summary - 36 years of IFIP. Edited by H. Zemanek, Laxenburg, IFIP.

Järvinen, P., (2000), Research Questions Guiding Selection of an Appropriate Research Method. Proceedings of the 8th European Conference on Information Systems (ECIS 2000), July 3-5, Vienna.

Lichtenstein, S. & Swatman, P.M.C., (1997), Internet acceptable usage policy for organizations. Information Management and Computer Security. Vol. 5, no. 5, pp. 182-190.

Lindup, K. R., (1995), A New Model for Information Security Policies. Computer & Security, Vol. 14, No. 8, p. 691-695.

Lupu, E. & Sloman, M., (1997), A Policy based role object model. Proceedings of the First International Enterprise Distributed Object Computing Workshop. IEEE Computer Society Press.

McLean, J., (1990), The specification and modelling of computer security. IEEE Computer. January, vol. 23, issue 1, pp. 9-16.

Poore, R. S., (1996), The Lowly Password. Information Systems Security. Vol. 7., No. 1.

Ross, D., (1930), The Right and the Good. Oxford University Press.

Sandhu, R., (1998), Role-Based Access Control. Advances in Computers, Vol.46, Academic Press.

Sandhu, R.S, (1993), Lattice-based access controls. IEEE Computer. Pp. 9-19.

Sandhu, R., & Samarati, P., (1994), Access Control: Principle and Practice. IEEE Communications vol. 32, issue 9, pp. 40-48.

Sibley, E.H., Wexelblat, R.L., Michael, J.B., Tanner, M.C., & Littman, D.C., (1993), The role of policy in requirements definition. Proceedings of the IEEE International Symposium on Requirements Engineering.

Spruit, M.E.M, (1998), Competing against human failing. 15th IFIP World Computer Congress. 'The Global Information Society on the Way to the Next Millennium'. SEC, TC11. Vienna.

Straub, D. W., (1990), Effective IS Security: An empirical Study. Information System Research. Vol. 1, Number 2, June, p. 255-277.

Straub, D.W. & Welke, R.J., (1998), Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, Vol. 22, No. 4, p. 441-464

Summers, R., (1997), Secure Computing: Threats and safeguards. McGraw-Hill.

Thomas, R.K. & Sandhu. R. S., (1994), Conceptual Foundations for a Model of Task-based Authorizations. Proceedings of the 7th IEEE Computer Security Foundations Workshop. Franconia, NH, June.

Truex, D.P., Baskerville, R. & Klein, H., (1999), Growing Systems in Emergent Organizations. Communications of the ACM. Vol. 42, No. 8, pp. 117-123.

Warman, A.R., (1992), Organizational computer security policy: the reality. European Journal of Information Systems. Vol. 1, no. 5, pp. 305-310.

Wood, C.C., (1995), Writing InfoSec Policies. Computer & Security, Vol. 14, No. 8, p. 667-674.

Wood, C.C., (1996a), Constructing difficult-to-guess passwords. Information Management & Computer Security. Vol. 4, no.1, pp. 43-44.

Wood, C.C., (1996b), A computer emergency response team policy. Information Management & Computer Security. Vol. 4, no.2.

Wood, C.C., (1996c), A Policy for sending secret information over communications networks. Information Management & Computer Security. Vol. 4, no.3.

Wood, C.C., (1997a), Part of the foundation for secure systems: separation of duties policy. Information Management & Computer Security. Vol. 5, no.1, pp. 18-19.

Wood, C.C., (1997b), A secure password storage policy. Information Management & Computer Security. Vol. 5, no.2, pp. 79-80.

Yialelis, N., Lupu, E., & Sloman, M., (1996), Role-Based Security for Distributed Object Systems. Proceedings of the 5th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'96).