Information Security Management Standards: Problems and Solutions

Mikko T. Siponen

Department of Information Processing Science, University of Oulu,
P.O Box 3000, 90014 Oulu University, Finland
Mikko.T.Siponen@oulu.fi

Abstract

This paper critically analyses the foundations of three widely advocated information security management standards (BS7799, GASPP and SSE-CMM). The analysis reveals several fundamental problems related to these standards, casting serious doubts on their validity. The implications for research and practice, in improving information security management standards, are considered.

Keywords

Information security management standards

Introduction

Security aspects have been neglected in information systems (IS)/software development methods (Baskerville 1993, Dhillon & Backhouse 2001). To overcome this weakness, several IS security methods have been proposed (Baskerville 1993, Dhillon & Backhouse 2001, Dhillon 1997, Siponen, 2001). Of these methods, security checklists and management standards (classified as normative management-oriented security standards) are widely used (Parker 1998, Eloff & Solms 2000a, b, Solms & Haar 2000). In fact, IS security journals, including Computers & Security, Information Systems Security, Information Management & Computer Security, and information security management conference proceedings (e.g., annual IFIP TC11), are saturated with articles by security practitioners and academics paying lip service to the various existing standards; see, for example, Eloff and Solms (2000b), Ferris (1994), Ferraiolo and Sachs (1996), Fitzgerald (1995), Hardy (1995), Hopkinson (2001), Pounder (1999) and Solms (1996, 1998, 1999). To boot, many even view these standards as the key issue in the business of security management (Eloff & Solms 2000a, Janczewski 2000). In the background, protests have been heard. Baskerville (1993) criticized checklists for not paying enough attention to the fact that organizations' security requirements differ. Dhillon and Backhouse (2001) see checklists as mechanistic and therefore as not paying adequate attention to the social nature of organizations. We would apply these objections to checklists equally to standards. With respect to standards, Parker (1998, p. 214-215) criticized GASSP (1993) as "folk art" for failing to include the viewpoints of deterrence and sanctions.

Nevertheless, it is unfortunate that we have not encountered any attempts by advocates of standards/checklists to reply to these criticisms. Given that one of the key elements of

academic research is its "self-corrective method" (Chalmers 1982, Niiniluoto 1990, 1999, Popper 1992), it is imperative that we offer constructive criticism to some of our colleagues in the academy, insofar they have failed to accomplish this important objective of scientific research. The purpose of this paper is to extend and deepen these criticisms by exploring specific problems of selected management-oriented information security standards; and, on the basis of this analysis, offering suggestions on how things may be improved.

This research effort is worthwhile for several reasons. First, scholars should be aware of the underlying theoretical foundations of different methods (e.g., Dhillon 1997, Dhillon & Backhouse 2001, Hirschheim et al. 1995), and particularly their possible weaknesses. As Lakatos put it: "monolithical domination or dogmatic acceptance of a paradigm is a symptom of pseudoscience…" (Metaxopoulus 1989, p. 204). Second, it is common knowledge that we humans reflect the different beliefs and kinds of knowledge imparted to us through our upbringing and education or acquired by personal experience (e.g., Hare 1952). Therefore, it is important to analyze critically the underlying assumptions of information security methods. In fact: "The game of science is, in principle, without end. He who decides one day that scientific statements do not call for any further test, and that they can be regarded as finally verified, retires from the game" (Popper 1985, p. 140). This paper also offers a practical contribution by unveiling the important limitations of the widely used security management approaches for practitioners. A preliminary version of the paper was presented at the Second Annual International Systems Security Engineering Conference (2001).

The rest of this paper is composed as follows. The normative standard approaches are introduced in the second section. These standards are outlined and analyzed in the third, the implications of these analyses are discussed in the fourth, and the key issues are summarized in the fifth section.

Normative standards

Different management standards exist, including TCSEC/Orange Book, GMITS, CobiT, IT Protection Manual, BS7799, GASSP, SSE-CMM, ITSEC (1990), CTCPEC, FC, CC, TNI, NCSC, EPL, TDI (see Abrams & Podell 1995, Chokhani 1992, Eloff & Solms 2000a). Some of these are more computer system- than organization oriented, such as the Common Criteria and the Orange Book, and are labelled as technical (Overbeek 1995). Organization-oriented security standards include GMITS, BS7799 (1993, 1999), the OECD guidelines, GASSP (1999) and the System Security Engineering Capability Maturity Model (SSE-CMM 1998a,b).

These organizational oriented standards differ in level of abstraction. They vary from loose frameworks for security management (e.g., GMITS), to a list of security imperatives, i.e., "do that/don't do that" (e.g., BS7799 1993, IT Protection Manual 1996), which resemble those in checklists (e.g., "users should use passwords that are more than eight characters long…") that add security to IS in a tick-in-the-box manner (Baskerville 1993). Moreover, maturity standards also have a social-level role, as they present the security "maturity" level of the organization (Siponen 2002).

Of these standards, we selected three - BS7799, GASSP and SSE-CMM - as examples for analysis on the basis of three factors. First, they are rather new; it would be unfair to criticize only security standards that are more than twenty years old. Second, they are widely (internationally) advocated by both practitioners and academic scholars. Third, their advocates are geographically separated. The standards are introduced below:

Generally Accepted Information Security Principles (GASSP)

GASSP (1999) proposes three levels of principles:

- pervasive (few, rarely changing) principles such as those of ethics and awareness;
- broad functional (more detailed than pervasive) principles; and
- detailed (most detailed) principles.

The International Committee of GASSP includes members from more than 10 countries (GASSP 1999, p. 30-31) but, for reasons unknown to us, GASSP has not emerged as an object of discussion in academic forums, unlike BS7799 and SSE-CMM (but see the special issue on GASSP in Information Systems Security, vol. 8, No. 3).

BS7799

The 1993 version of BS7799 has received the greatest attention - and has been praised to the skies in various academic forums (e.g., Solms 1998). This is therefore the one chosen for the present analysis (although we also discuss the 1999 version where relevant). BS7799 has its academic advocates in Australia, South-Africa and the UK. BS7799 (1993) suggests abstract controls, practices or procedures that should be implemented. However, one could also use it for the purpose of analyzing the level of maturity of a system. In that case, a mature security system would be one that meets a certain amount of the principles described by standards.

System Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM (1998) is used most in North America, where its roots lie. It started in 1993 as a NSA-sponsored endeavour to extend the Capability Maturity Model (cf., Herbsleb *et al*. 1997, Paulk *et al*. 1993, Shere & Versel 1994) in the field of software engineering to address security matters. Thereafter, SSE-CMM-dedicated workshops and conferences have been held in North America that have aroused wide interest among practitioners. SSE-CMM is now a well-organized effort. It includes 22 process areas (11 security-related and 11 general project-oriented) and five maturity levels. The SSM-CMM can be used for 1) evaluating (the maturity level of) a system's security; and 2) improving the security of systems – or, more precisely, their security processes. We have chosen SSE-CMM as representative of the various security maturity approaches as it is most well-known and it is more systematically developed than its "competitors" (cf., Siponen 2002).

Management and maturity standards can be included in the category of IS security development methods since they are prescriptive (e.g., in relation to improving processes or systems); see figure 1.

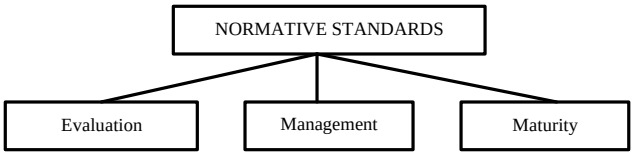

Figure 1. Normative standards

BS7799, for example, is called a management standard because it provides an aid for managers to ensure that certain issues or aspects are "properly" taken into account. Given that standards suggest safeguards or countermeasures, they guide development. Hence, the label

"normative standards". Maturity and management standards therefore also have a role similar to that of traditional development standards (e.g., checklists); see figure 1.

The term management standard is in fact misleading since security standards present a list of controls/procedures at different levels of abstraction which should then be implemented. "Management", however, encompasses activities that are much more complex than just the insertion of a list of controls suggested by the standard (cf., Bartol & Martin 1994). In fact, such standards do not provide any help concerning real management problems stemming from the application of the standard, such as managerial decision-making (cf., Baskerville & Siponen 2002).

Critical Analysis of the Normative Standards

There are four problematic assumptions commonly made in the standards: "is from ought", irrationalist research process and the inference problem.

"Is from Ought"

The standards take certain (industrial) practices as their point of departure and suggest that organizations should follow these practices. Thus, the standards suggest that the actions that organizations should take in order to secure their IS can be derived from prevailing industrial practices. This can be seen in the following extracts:

GASSP: "practices are generally accepted because they represent prevalent practice in a particular industry" (GASSP 1999, p. 33), and likewise the SSE-CMM "is a compilation of the best-known security engineering practices" (SSE-CMM, 1998). Best-known practices means that security experts have achieved a consensus on what the standards should include (Hopkinson 2001). BS7799 is no exception: "These generally accepted controls are often referred to as baseline security controls, because they collectively define an industry baseline of good security practice" (BS7799 1993, p. 1). These statements suggest that the standards are constructed by observing the prevailing industrial practice. More importantly, these extracts indicate that the prescriptions contained in the standards are valid, simply because they present an existing industrial practice (e.g., consider the above passage by GASSP). However, this is the wrong way of doing things. The fact that something (X) can be done – or some organizations are doing X – does not imply that other organizations should therefore do X. Hence, they propose "ought" conclusions (what organizations should do) from "is" premises (what an organization does).

Naive inductionism

Normative standards are at best based on naive inductionism (cf., Chalmers 1982). They presume that there are certain universal solutions, i.e., solutions that are valid regardless of environment and situation (cf., Baskerville 1992). These solutions are first observed, e.g., in sales catalogues, conference proceedings or organizations. Then, at best, they are validated by singular observations made in a certain environment at a certain time, such as the observation that a certain solution (e.g., packer-filter firewall) reduced the amount of electronic break-ins (hacking) in a certain period of time in a given environment (example 1). This observation is then universalized. The weakness is that even if singular observations are reliable, it does not follow that they can be either generalized or universalized. This is termed "naive inductionism". Consider this example with respect to generalization: "some controls [which the code of practice suggest] are not applicable to every IT environment and should be used

selectively. However, most of the controls documented are widely accepted..[and]…recommended good practices for all organizations" (BS7799 1993).

With respect to universalization, BS7799 prescribes key controls, which "are either essential requirements…or are considered to be fundamental building blocks for information security." (BS7799 1993 p. 2). BS7799 states that these controls "apply to all organizations and environments" (BS7799 1993, p. 2), i.e., they are universal.

However, even if a firewall reduced hacking activities, say by 55 percent and saved a million dollars in a certain organization (and for that reason the particular firewall was justified), it does not follow that it would do the same in every organization.

It follows from the weaknesses of "from is to ought" and naive inductionism that standards may not pay enough attention to organizational differences, but instead suggest that certain solutions or procedures are valid for each and every organization. As the example above shows, BS7799 falls into this trap by advising implementation of all the key controls

At first sight GASSP and SSE-CMM seem to skirt the "universal" fallacy – the second "stage" of naive inductionism – better than BS7799. GASSP distinguishes between what is "generally accepted" and "universally accepted" and notes that "all principles may have exceptions" (GASSP 1999, p. 34). Thus it seems to recognize this problem but, even more importantly, it does not give any advice on how to recognize and make these exceptions.

SSE-CMM seems to recognize that organizations' security requirements differ. It does this by forming process areas: "The SSE-CMM does not prescribe a particular process or sequence, but captures practices generally observed in industry" (SSE-CMM, 1998). Closer inspection reveals, however, that I) the process areas are predefined and universal, so that the same process areas should be found and applied in every organization, and II) the five maturity stages are fixed in advance and universal, which gives the SSE-CMM's maturity criterion a strong flavour of naive inductionism, as experts' singular-type observations are universalized. This means in practice that even it were true that a few organizations improve their systems' security when they increase maturity in accordance with SSE-CMM – which we do not know, as no proper evidence has been presented so far – it does not imply that this is valid for all organizations. For example, SSE-CMM may certainly advocate process areas for which a small organization will not have the relevant security needs. Thus, in order to follow SSE-CMM literally, one may have to build too much security, which is costly among other things. The same goes for increasing the maturity level – as it may even harm the organization as well. Note that although the objection "of course practitioners are not stupid - one can just bypass this particular point" is true, in order to achieve a certain maturity level (e.g., in order to increase the organizations' status in the eyes of customers and business partners), small organizations have to follow SSE-CMM to the letter (even though it may be totally irrelevant and perhaps even detrimental to them).

Irrationalist research process

The main reason why the existing standards may not be based even on naive inductionism is that the observation and underlying research processes are not considerable and the results are not duplicable. The authors of standards have not allowed for the possibility of checking the validity either of singular observations (perhaps because such information may be considered too sensitive), or of the underlying research process. This means that normative standards are ultimately based on A) "measured" results; or B), more likely, the authors' subjective experiences about what can be done. Consider GASSP, for example: "the principles have been developed on the basis of experience, reason, custom…" (GASSP 1999).

Both A and B are problematic. When it comes to "measuring" (A), normative standards do not offer exact information about the measuring process nor its results, so that its reliability (or objectivity) cannot be evaluated. BS7799 (1993), for example, validates the controls by saying that "most of the controls documented are widely accepted by large, experienced organizations as recommended good practices for all situations". As for the other standards (GASSP and SSE-CMM), we have already presented similar extracts in section 3.2.1). Irrationalism comes into play as it is unknown how reliable such information is. It is not known how such a statement (the extract from BS7799 above) is experienced. It is questionable whether any research method has been used to obtain the results. At least, we do not know what scientific research methods have been used. SSE-CMM and GASSP insinuate that there have been none at all. SSE-CMM states that the standard is based on experts' judgments based on their personal experiences (Hopkins 2001). GASSP (1999) follows a similar approach: "they [principles] become generally accepted by agreement (often tacit agreement) rather than formal derivation from a set of postulates or basic concepts" (GASSP 1999, p. 33). BS7799 does not say what "accepted by large organizations" means, or on what criteria they regard something as "accepted" (the extract from BS7799 above). Moreover, there are several other questions that are left unanswered, including: Are there better solutions? Why is this particular solution/procedure that the checklists/normative standards favour better than the other possible solutions? Why it is good for all situations?

To see what these weaknesses may mean in practice, let us return to the above example concerned with the efficiency of firewalls. In scientific terms, we are not certain whether the firewall is the only causal hypothesis in the example. It may be a case of Complex Cause, i.e., the effect, a reduced number of security violations, is caused by several circumstances, of which the firewall is only one. Given that such a situation exists – that because there are other causal factors that are unknown, only the firewall is recognized as the cause- leading to the effectiveness of firewalls being universalized or generalized, we are confronted with a coincidental correlation. It may be, for example, that the watchfulness of staff increased due to these measurements, and perhaps the activity as a whole (firewall + measuring) functioned as a deterrent. Or perhaps the period was just quieter generally in terms of security violations, etc. Both are examples of possible reasons for a reduction in security violations – and no attempt is made to rule out such reasons.

The alternative (B), in which the normative standards are based on personal observations, is also problematic. Namely, personal feelings and experiences per se are inadequate as sources of validation in cases where the possibilities exist for the application of more reliable research approaches (Chalmers 1982), although some extreme relativists and method anarchists, such as Feyerabend (1964), may be ready to accept them as valid methods. First, it is difficult to separate our beliefs and expectations, etc. from observation, and we err. Realists (e.g., Holton 1994, Lakatos 1970, p. 175, Metaxopoulus 1989, Musgrave 1993, Popper 1992, Niiniluoto 1999) agree with us in this respect. Second, it is not very persuasive to answer the question "Why this? Why not something else?" by saying "Because I feel this way!" without any further information. Third, anti-realists may in any case not accept B. Even an irrational philosopher of science, such as Feyerabend-the-anything-goes (cf., Preston 2000, Chalmers, 1982), would not accept the way normative standards are developed: "a crank…is not at all prepared to test its usefulness in all those cases which seem to favour the opponent, or even to admit that a problem exists. It is this further investigation, the details of it, the knowledge of difficulties, of the general state of the knowledge, the recognition of objections, which distinguishes the respectable thinker from the crank." (Feyerabend 1964, p. 305). So, to be a serious thinker, two conditions should be met: there must be a) a willingness to test; and b)

the recognition of objections. Even on Feyerabend's criteria, the developers of standards seem to be more "cranks" than "respectable thinkers". They are not keen to publish their observations (or the data and processes behind those observations) nor to test their work further. Furthermore, "the recognition of objections" as a condition is not met, given that the checklists/normative standards do not take into account related work, not even relevant objections or the use of relevant research methods.

The inference problem

Normative standards may also involve an inference problem, which is argued to be a "fundamental problem in computer security" (see Garvey 1992). Consider, for example, an organization that builds its security using Baseline controls (as suggested by Parker 1998). The Baseline approach compares the safeguards of a target organization with those of its peers in the same industry, and if the target organization does not meet the "due care" standards for the industry, then these baseline controls should be implemented. The baseline approach is therefore similar to security management (normative) standards, in that certain standards should be met regardless of organizational and environmental differences. The inference problem may manifest itself as a person knowing the vulnerabilities of such controls, e.g., areas that the standards do not cover adequately, who would then know the weak points of organizations that use such standards (Parker 1998, p. 214-216, for example, has reported several issues that the GASSP standard does not cover).

Discussion, the limitations and implications of this study

This paper analyzed three widely used and advocated standards: BS7799, GASSP and SSE-CMM.

These standards succumb to the "Is-Ought" fallacy. The fact that some organizations do X does not imply that all organizations should do X. This is because normative security standards do not start by addressing the organization's own, perhaps unique, security needs, but prescribe universal or general procedures advocated by security practitioners. Furthermore, compliance with existing practices upholds conventionalism, which is problematic in the long-run, given that it leads to reactionary attitudes and prevents innovations. Therefore, top companies wanting to use security as a competitive edge, or otherwise seeking innovations in terms of security, do not find normative standards very useful. The 1999 version of the BS7799 has moved in the right direction by stating that standards can be used as a starting point for developing organization-specific guidelines (BS7799 1999). However, using BS7799 as a starting point will not ensure that organizations' specific security requirements are met (the organizations' own security requirements should be the starting point).

The normative standards seem to be based on naive inductionism by generalizing or universalizing a singular subjective observation. However, even if a singular observation is reliable, it does not guarantee that the observation can be universalized. Nevertheless, if normative standards, e.g., "key controls" in BS7799, were universally valid (valid in every organization) they would be highly falsifiable, i.e., we could put them to the test and see whether they would work perfectly in every organization. As already mentioned, a very small organization may be harmed by implementing all the controls and procedures specified in these three standards. It is highly questionable, for example, whether the key controls in

BS7799 are relevant to all situations (from a company with two PCs to large multinational corporations).

Normative standards are not validated seriously enough, but rather they reflect their developers' own preferences and personal experiences. Such a research process can be labelled irrationalist in terms of the philosophy of science, as it suggests that academically accepted research methods do not count for anything, but that one may instead rely on intuitions (e.g., Mautner 1996, p. 215). Irrationalism is highly problematic. The fact that we trust in our intuitions and observations in cases where more reliable research approaches would have been available has detrimental effects on research and practice. Research cannot be seriously validated on the basis of intuitions and naive inductionism - the risks from counting on them are too high – particularly more reliable research paradigm exits! These weaknesses mean in practice that we have no evidence concerning the reliability of such standards. In the case of a maturity standard, for example, one cannot be sure that the maturity level truly reflects the real security maturity of the systems. Thus any process improvement suggestions may not be optimal. Consequently, it is crucial to know is why X is done, what its real effects and implications are, and to what extent such findings can be generalized (if at all), etc. Current standards fail to pay any attention to these vital aspects.

The normative standards might be confronted with an inference problem, meaning a situation in which a malicious person who knows that a certain organization abides by given standards might be able to infer areas that the standard and the organizations following it will not render sufficiently secure.

Further research is needed to overcome these problems. Rigorous empirical studies over a wide cross-section of data are needed in which 1) neither the research process nor the results are secret, and 2) (all) the possible variables are considered. Thus, the authors of such standards should 1) try to validate their real usefulness and implications empirically, and 2) consider, on the basis of 1, what environments and organizations may be relevant. Scientific theories and research methods (see Järvinen 1997, 2000, Jenkins 1985, Galliers & Land 1987, Iivari 1991, Nunamaker *et al*. 1991, Stohr & Konsynski 1992, Henne & Moller 1995, March & Smith 1995), provided that they have survived scientific inspection, are in all probability more reliable than an individual's personal experiences, presumptions, intuitions and speculations (Popper 1992, Niiniluoto 1999). Both quantitative (e.g., action research, interpretive field studies, interpretive case research) and qualitative studies (e.g., survey) forming two research streams are required. In the first stream, there is a need to study what security techniques and methods organizations use and what the real effects and possible weaknesses of these methods are in practice. The methods and techniques prescribed by standards should be based on such results. In the second stream, studies are needed - not just to study individual techniques - but the perceived usefulness, ease of use (cf., Davis 1989) as well as problems and implications of the utilization of whole standards in real organizations. Moreover, research is needed to study how these standards can be integrated into normal system development or management activities (Baskerville 1992).

More care should be paid to the generalizability of the findings in particular. When developing new standards, it the extent to which the existing results can be generalized should be carefully considered; in other words, to what organizations they may have relevance. Put more scientifically, to avoid naive inductionism and irrationalism, it is suggested that probability induction within a research programme (cf., Lakatos 1970) could be used as the guiding foundation for developing a normative standard. Owing to this probability induction, empirical evidence that supports the relevance of the particular

checklist/normative standard in certain environments will increase the likelihood, or confidence, that the checklist/normative standard may be relevant in a similar environment. We can combine this with a hypothetical-deductive approach, such as modified versions of falsificationism, to perceive the limits of the standards/generalizations. We do not mean by this that the hypothetical-deductive process is able refute the whole relevance of a standard (as would be in the case with traditional Popperian falsificationism), but that it can show the limits of the standards/statistical generalizations. Following this idea, the development of standards may be seen as a research programme (cf., Lakatos 1970, Loose 1993).

Summary

Management (e.g., BS7799, GASSP) and maturity (e.g., SSE-CMM) standards as well as checklist can be regarded as development-guiding - normative – standards. Maturity and management standards play a similar role to that of traditional development standards such as checklists. The analysis of the three normative standards revealed several weaknesses. First, normative standards are claimed to be, if not universally valid, at least generally valid. Second, they are based on exploring "is" matters (what forms of protection are available, or what is done in other organizations), the norms (standards) for which are then universalized. The fallacy is that what is done in an organization does do not *per se* allow us to deduce what other organizations should do (Hume's Law "no ought from an is"). Moreover, normative standards are based on unjustified personal observations (derived from limited material), speculations and might include an inference problem. The major implication of this research is that normative standards in their current forms are questionable. It is suggested that the normative standards should favor a more reliable development philosophy instead of naive inductionism. A possible, and perhaps more reliable, approach would be one based on research programs.

References

Abrams, M.D., & Podell, H.J., (1995), Evaluation Issues. In: Information Security - An Integrated Collection of Essays, Edited by M. D. Abrams, S. Jajodia & H. J. Podell, IEEE Computer Society Press, Los Alamitos, CA, USA.

Bartol, K.M. & Martin, D.C., (1994), Management. International edition. McGraw-Hill, inc.

Baskerville, R., (1992), The Developmental Duality of Information Systems Security. Journal of Management Systems. Vol. 4, no. 1, pp. 1-12.

Baskerville, R., (1993), Information Systems Security Design Methods: Implications for Information Systems Development. Computing Surveys 25, (4) December, pp. 375-414.

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

Caplan, K. & Sanders, J.L., (1999), Building an international security standard. IT Professional, vol. 1, no. 2, March-April, pp. 29–34.

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

Chokhani, S., (1992), Trusted products evaluation. Communications of the ACM. Vol. 35, Issue 7, pp. 64-76.

Code of Practice for Information Security Management, (1993), Department of Trade and Industry. DISC PD003. British Standard Institution, London, UK.

BS7799-1, (1999), Code of Practice for Information Security Management, Department of Trade and Industry.

Davis, F., (1989), Perceived usefulness, perceived ease of use, and acceptance of information technology. MIS Quarterly, Vol. 13, no. 3, September, pp. 319-340.

Dhillon, G., (1997), Managing Information Systems Security. MacMillan Press LTD, UK.

Dhillon, G. & Backhouse, J., (2001), Current directions in IS security research: toward socio-technical perspectives. Information Systems, Vol 11, No 2.

Eloff, M.M. & Solms, S.H., (2000a), Information Security Management: A Hierarchical Framework for Various Approaches. Computers & Security, Vol. 19, pp. 243-256.

Eloff, M.M. & Solms, S.H., (2000b), Information Security: Process Evaluation and Product Evaluation. Sixteenth Annual Working Conference on Information Security, Beijing, China.

Ferraiolo, K., & Sachs, J.E., (1996), Distinguishing Security Engineering Process Areas by Maturity Levels. Proceedings of the 9th Annual Canadian Information Technology Security Symposium.

Ferris, J.M., (1994), Using Standards as a Security Policy Tool. ACM Standard view, vol. 2, no. 2, pp. 73-77.

Feyerabend, P., (1964), Realism and Instrumentalism: Comments on the logic of Factual Support. In M. Bunge (eds): The Critical Approach to Science and Philosophy. Free Press, New York, USA.

Fitzgerald, K.J., (1995), Information security baselines. Information Management & Computer Security, Vol. 3 Issue 2, pp. 8-12.

Galliers, R.D., & Land, F.F., (1987), Choosing appropriate information systems research methodologies. Communication of the ACM, vol. 30, no. 11, pp. 900-902.

Garvey, T.D., (1992), The Inference Problem for Computer Security. Proceedings of the Fifth Computer Security Foundations Workshop. IEEE Computer Society Press.

GASSP, (1999), Generally Accepted System Security Principles (GASSP). Version 2.0. Information Systems Security. June, vol. 8, no. 3.

Hare, R. M., (1952), The Language of Morals. Oxford University Press, Oxford, UK.

Hardy, G., (1995), Standards - The Need for a Common Framework. Computers & Security, Vol. 14, Issue 5, pp. 426-427.

Henne, A. & Moller, E.M., (1995), Innovation in business processes-a discussion of research methods to study the process of innovation. Proceedings of the Twenty-Eighth Hawaii International Conference on System Sciences, Vol. V, IEEE Computer Society Press.

Hirschheim, R., Klein, H. K., & Lyytinen, K. (1995). Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations. Cambridge University Press, UK.

Holton, G., (1994), Science and Anti-Science. Harvard University Press, Cambridge, Massachusetts, USA.

Hopkinson, J.P., (2001), Security Standards Overview. Proceedings of the Second Annual International Systems Security Engineering Conference.

Iivari, J., (1991), A paradigmatic analysis of contemporary schools of IS development, European Journal of Information Systems, Vol. 1, No. 4, pp. 249-272.

Information Technology Security Evaluation Criteria (ITSEC) (1990), Harmonised Criteria of France, Germany, the Netherlands and the United Kingdom.

IT Baseline Protection Manual, (1996), BSI, Germany.

Janczewski, L., (2000), Managing Security Functions Using Security Standards. In L. Janczewski (eds): Internet & Intranet Security Management: Risks and Solutions, Idea Group Publishing, USA, pp. 81-105.

Jenkins, M.A., (1985), Research methodologies and MIS research. In E. Mumford et al. (eds.): research methodologies in information systems. Elsevier Science Publishers B.V., pp. 103-117.

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.

Herbsleb, J., Zubrow, D., Goldenson, D., Hayes, W., Paulk, M., (1997), Software Quality and the Capability Model. Communications of the ACM, vol. 40, no. 6, pp. 30-40.

Lakatos, I., (1970), Falsification and the Methodology of Scientific Research Programmes. In I. Lakatos and A. Musgrave (eds): Criticism and the growth of knowledge. Cambridge University Press, UK.

Loose, J., (1993), A Historical Introduction to the Philosophy of Science. Third Edition, Oxford University Press, Oxford, UK.

March, S.T., & Smith, G.F., (1995), Design and natural science research on information technology. Decision support systems, 15, pp. 251-266.

Mautner, T., (1996), A Dictionary of Philosophy. Blackwell Publishers Ltd, Oxford, UK.

Metaxopoulos, E., (1989), A Critical Consideration of the Lakatosian Concepts: "Mature" and "Immature" Science. In K. Gavroglu, Y. Goudaroulis and P. Nicolacopoulos (eds): Imre Lakatos and Theories of Scientific Change, pp. 203-214, Kluwer Academic Publishers.

Musgrave, A., (1993), Common Sense, Science and Sceptism. Cambridge University Press, UK.

Niiniluoto, I., (1990), Science and Epistemic Values. Science Studies (3:1):21-25.

Niiniluoto, I., (1999), Critical Scientific Realism. Oxford University Press, Oxford, UK.

Nunamaker, J.F., Chen, M., Purdin, T.D.M., (1991), Systems development in information systems research. Journal of Management Information Systems, vol. 7., no. 3., pp. 89-106.

Overbeek, P.L., (1995), Common Criteria for IT Security Evaluation - Update Report. Proceedings of the IFIP TC11 Eleventh International Conference on Information Security, IFIP/SEC'95.

Parker, D. B., (1998), Fighting Computer Crime - A New Framework for Protecting Information. Wiley Computer Publishing. USA.

Paulk, M.C., Curtis, B., Chrissis, M.B, Weber, C.V., (1993), Capability Maturity Model. Version 1.1. IEEE Software, Vol. 10, issue 4, pp. 18-27.

Popper, K., (1985), Scientific Method. In: Popper Selections (eds): D. Miller, Princeton University Press, USA, pp. 133-142.

Popper, K.R, (1992), In Search of a Better World: Lectures and Essays from Thirty Years. Routlege, London, UK.

Pounder, C., (1999), The Revised version of BS7799-so what's new? Computers & Security, vol. 18, issue 4, pp. 307-311.

Preston, J., (2000), Feyerabend. In W.H. Newton-Smith (eds): A Companion to Philosophy of Science, Blackwell Publishers, UK, pp. 143-148.

Shere, K.D. & Versel, M.J., (1994), Extension of the SEI software capability maturity model to systems. Proceedings of the Eighteenth Annual International on Computer Software and Applications.

Siponen, M.T., (2001), An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In G. Dhillon (eds:) Information Security Management - Global Challenges in the Next Millennium. Idea Group Publications, Hershey, PA, USA, pp. 101-124.

Siponen, M.T. (2002): Towards Maturity of Information Security Maturity Criteria: Six lessons learned from software maturity criteria. Information Management & Computer Security, vol. 10, no. 5, pp. 337-436.

Solms, R., (1996), Information security management: The Second Generation. Computers & Security, vol. 15, no. 4, pp. 281-288.

Solms, R., (1998), Information security management (3): the Code of Practice for Information Security Management (BS 7799). Information Management & Computer Security. Vol. 6, Issue 5, pp. 224-225.

Solms, R., (1999), Information security management: why standards are important. Information Management and Computer Security, Vol. 7, Issue 1, pp. 50-58.

Solms, R., & Van Der Haar, H., (2000), From Trusted Information Security Controls to a Trusted Information Security Environment. Information Security Sixteenth Annual Working Conference on Information Security, Beijing, China.

SSE-CMM, (1998a), The Model. v2.0. http://www.sse-cmm.org.

SSE-CMM, (1998b), The Appraisal Method. v2.0. http://www.sse-cmm.org.

Stohr, E.A. & Konsynski, B.R., (1992), Research Approaches in ISDP. Information Systems and Decision processes, Stohr, E.A. & Konsynski, B.R (eds.). IEEE Computer Society Press, Los Alamitos, CA, USA.