7

MATURITY CRITERIA FOR DEVELOPING SECURE IS AND SW

Limits, and Prospects

Mikko T. Siponen
University of Oulu, Department of Information Processing Science, Linnanmaa, P.O.BOX 3000, FIN-90014 Oulun yliopisto, FINLAND. E-mail:Mikko.T.Siponen@oulu.fi

Abstract: Traditionally, information security management standards listing generic means of protection have received a lot of attention in the field of information security management. In the background a few information security management-oriented maturity standards have been laid down, albeit they have been elided by the information security community in great measure. The aim of this study is to analyze the alternative maturity criteria - SSE-CMM, Security Program Maturity Grid, Software Security Metrics - for developing secure IS/software (SW). First, a framework synthesized from the information systems (IS) and software engineering (SE) literatures is advanced. Secondly, the existing information security maturity criteria are pored over in the light of this framework. Thirdly, on the basis of results of this analysis, implications for practice and research are presented.

Key words: Information Systems Security, information security management.

1. INTRODUCTION

A few studies suggest that the alternative methods for developing and managing secure IS are influenced by the IS/SW development methods of previous generations (Baskerville, 1993; Dhillon & Backhouse, 2001; Siponen, 2001; Siponen & Baskerville, 2001). It is interesting that perhaps the oldest approach, namely checklist-standard-based securing of IS (Baskerville, 1993), has continued to exist. Even though the checklists are not a hot topic in the contemporary information security literature, their cognate method – security management standards (cf. Baskerville, 1993;

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: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

Dhillon & Backhouse, 2001; Siponen, 2001; Siponen & Baskerville, 2001) – have received increasing attention from both information security researchers and practitioners (Eloff & Solms, 2000a; Eloff & Solms, 2000b; Fitzgerald, 1995; Hopkinson, 2001; Janczewski, 2000; Solms, 1998; 1999). Information security management standards can be regarded as a legacy of checklists. Both (checklists and management standards) offer a ready-made generic catalogue of protection means (Baskerville & Siponen, 2002), fabricated rather by the experiences of practitioners than the results of academic research. Recently, following ideas and developments in the field of SE (e.g. Pfleeger et al., 1994), a few information security management-oriented maturity standards have seen the light of the day. Recognizing this analogy in the field of SE, we see that information security maturity standards are the latest descendant of the information checklists-management standard genealogy.

Of all the standards targeted at management-level in the field of information security (cf. Eloff & Solms, 2000a), BS7799 has received the greatest interest, at least measured in terms of the sheer number of conference and journal articles. Utilizing the same gauge, it is strange that the existing information security management-oriented maturity approaches such as SSE-CMM, 1998; Murine-Carpenter, 1984; Stacey, 1996), have been not received similar attention. This is all the more strange given that the maturity ventures are currently the latest evolution of the checklists-management standard concept. In the field of SE, the respective maturity paradigm has received a lot of positive (Paulk et al. 1993) and negative attention (Bollinger & McGowan, 1991; Pfleeger, 1999; Rifkin, 2001; Voas, 1999). The aim of this study is to analyse the existing information security maturity criteria. The existing critiques of SE maturity models, in particular, provide good lessons on the problems of maturity endeavours, and we shall scrutinize the alternative information security maturity approaches using these lenses.

The rest of the paper is composed as follows. The second section provides an overview of the alternative maturity approaches and presents the framework for this study. The third section analysis the alternative information security management-oriented maturity standards. The fourth section discusses the findings of the paper while also proposing future research directions and questions which maturity standards should meet. The fifth section concludes summarizing the key contributions of the paper.

2. AN OVERVIEW OF THE ALTERNATIVE MATURITY APPROACHES AND THE FRAMEWORK FOR ANALYSIS

The following three information security management-oriented maturity approaches are introduced next. *SSE-CMM* is a cognate of the Capability Maturity Model (CMM) and ISO SPICE, both (CMM, SPICE) used to determine and improve the maturity of SW processes in SW houses with the help of five maturity levels (cf. Paulk et al. 1993). The first version of SSE-CMM appeared in 1994 and the current, second version, in 1998 (SSE-CMM, 1998), which is the version considered in this analysis. SSE-CMM has received attention only among North American scholars and practitioners (cf. Hefner, 1997; Hopkinson, 2001; SSE-CMM, 1998). SSE-CMM, like CMM, put forward five maturity stages where the first stage denotes the lowest level of maturity. Each stage consists of a fixed number of security processes (a sequence of steps performed to achieve a certain objective), i.e. security activities, which the organization should meet. To determine the maturity level of an organization, these security processes are trawled through in the form of a questionnaire consisting of "yes/no/don't know" questions within 22 process areas (such as PA03: assess security risk; PA12: ensure quality). Yet, SSM-CMM includes the concept of exploratory (free-form) questions to resolve possible inconsistencies and unsupported answers from questionnaires. SSM-CMM consists of two parts, a model (consisting of five maturity levels, as mentioned) and an appraisal method. The latter is a four-phased (planning, preparation, on-site, reporting) method with which to conduct the evaluation of organizations' maturity on the basis of SSM-CMM model.

Stacey's (1996) *Information Security Program Maturity* Grid also stems from the CMM. As in the case of SSE-CMM, Stacey proposes five stages in order of increased maturity: 1) uncertainty (a total lack of understanding of information security – security is a hindrance to productivity), 2) awakening (realization of the value of security, but inability to provide resources and money for security), 3) enlightenment (security is a must – as well as resources and money for security – organizations need also to prevent violation, instead of merely recovering from incidents), 4) wisdom (security development reflects organizations' environmental factors and needs – all users are empowered in terms of information security), and 5) benevolence (continuous security process improvement through research and practice). Also, like SSE-CMM, Stacey's method incorporates several more detailed principles associated with each maturity level.

Murine-Carpenter maturity criterion. The incentive behind the maturity criterion of Murine-Carpenter (1984) lies in building quantifiable metrics for

the information security maturity of systems and SW (Murine-Carpenter, 1984 p. 208). They feel that SW quality metrics do not address the security aspect adequately enough, resulting in the need to elaborate SW security metrics. They list 11 high-level security criteria (Murine & Carpenter, 1984 p. 212) and five milestones (Murine & Carpenter, 1984 p. 213), i.e. phases in SW development where the maturity of security in SW development should be analyzed in the light of their maturity criteria.

A framework for analysis: six viewpoints

Maturity endeavours started in the field of SE. The US Department of Defense (DoD) misjudged the ability of several its contractors to develop mature SW with the result that DoD deemed it imperative to mobilize a maturity standard (Bollinger, & McGowan; 1991; O'Connell & Saidian, 2000 p. 28). Not surprisingly, also critiques have been levelled against software process maturity standards. We find the following six recognized problems of existing SW maturity approaches.

Operational focus. Rifkin (2001) recognized that SW maturity criteria focus on operational issues alone. In fact, the SW maturity criterion does not support innovation at all, since it does not encourage organizations to innovate, but instead insists on the use of existing and well-known methods and practices. Rifkin (2001) therefore reported that organizations regarding innovation as their main competitive strategy gain nothing from the adaptation of SW maturity criteria. Also, organizations using very state-of-the-art security solutions, perhaps even participating in the creation of new security contributions, may not rank high in maturity estimations, as the new solutions are not recognized by the maturity criteria (as the criteria is based on old information).

The *naturalistic-mechanistic* view refers to the idea that phenomena can be quantified and controlled. Positivism, which claims that the methods of natural sciences should form the basis of all sciences, is the most well-known example of this view (cf. Hirschheim, 1985; Ray, 2000). Also, so-called behaviorists in the field of the behavioral sciences advocated a similar view, although with inferior results. When it comes to SW development, Humbrey (1988) states several hints giving impression that he is a proponent of this view. To provide examples, Humbrey sees that the SW process should be "predictable" (Humbrey, 1988 p. 73), predefined, repeatable (Humbrey, 1988 p. 74) and stable (Humbrey, 1988 p. 75). The aforementioned objectives, namely predefined, repeatable and predictable accord well with this scientific posture, as it leans on the paradigm of positivism. It is, however, an erroneous to contend that such a view of natural science is valid in all areas of science (i.e. positivism). The fallacy lies on the fact that the naturalistic-mechanistic view may be partially valid

in the arena of the natural sciences. However, this is not the case in the social or humanistic sciences. At least currently, human behavior cannot be deduced from specific causal reactions. If someone were able to this, there would most likely be no need for information security, as we would be able to manipulate or induce the necessary causal reactions with the result that people would not commit security violations. Advocates of SW maturity models may try to avoid this objection by saying that the SW can be developed within the research paradigm of natural sciences/positivism. The next quotation illustrates this view. Humbrey argues that "*while there are important differences, these concepts* [maturity, statistical process control] *are just as applicable to SW as they are to automobiles, cameras, wristwatches, and steel. A SW development process that is under statistical control will produce the desired results within anticipated limits of cost, schedule and quality.*" (Humbrey, 1988 p. 74). Such a viewpoint entails problems, however. Voas (1999 p. 120) put forward a rebuttal to Hubrey's claim, pointing that SW development is an inventive process; it is not a manufacturing process (as assumed in the citation from Humbrey). Pfleeger has pointed out that SW maturity criteria have relied upon the natural science (cf. Harré, 2000) conception of science: "*we* [SE people] *seek relationships to help us understand what makes good SW. We then apply what we learn so that we get good SW more often. Our search is based in large part on the notion of cause and effect.*" (Pfleeger, 1999 p. 33). Pfleeger further remark that this idea of "cause and effect" is fallacious because the processes are not natural, but human made, i.e. social processes. Nevertheless, even if one still insists that SW can be developed on the basis of the natural science paradigm, the problem with respect to security maturity criteria remains that these models – at least SSE-CMM and Information Security Program Maturity Grid – are applied to secure systems, not just secure SW development. Hence, even if the naturalistic-mechanistic view would be adequate for SW development, it is definitely not an adequate framework for approaches aimed at securing organizations' ISs.

Stable versus emergent organization structures and functions

SW maturity standards seem to imply that the IS/SW development takes place in a stable environment, for two reasons. First, current SW maturity models rely on strict waterfall models (Boehm, 2000). Secondly, they stem from the analogy cited from Humbrey between SW development and manufacturing, which, however, is argued here to be a mistake. This analogy is flawed since traditional manufacturing is largely stable and fine-tuning replication process, whereas SW development is more a creative design process (Bollinger & McGowan, 1991 p. 36). The some goes for IS development: recent studies support this argument and further aggravate this problem (stable manufacturing versus creative, and non-repeatable, design

process). For example, increasing numbers of organizations are reported to be emergent (as opposed to stable) in terms of their business environment, and hence they require appropriate means for developing SW/IS as the current IS/SW development methods are suited to stable organizations (Baskerville & Pries-Heje, 2001; Truex et al., 1999, 2000). They basic claim is that any modern IS/SW development method should support the requirements posed by emergent organizations, i.e. a successful method should be able to adapt rapidly to ever-changing requirements owing to a fast-paced business environment.

Double standard. Companies may be under a pressure to perform well in terms of maturity as a good maturity rating results in good publicity and an increase in business competence (O'Connell & Saidian, 2000 p. 32-33). The double standard refers to a situation where an organization manipulates its results in order to look better in a maturity evaluation. O'Connell & Saidian (2000 pp. 33-34) describes several such tricks that organization may play. Moreover, Bollinger & McGowan reported how maturity evaluators schooled by DoD are trained to "*distinguish genuine answers from attempts at obfuscation or even outright falsification.*" (Bollinger & McGowan, 1991 p. 28). They also provide a few countermeasures for this problem, including conducting online empirical evaluations (not just paper-based), requiring two sources of confirmation, choosing a representative evaluation team. However, is it clear that these proposed cures do not remove these problems.

The problem of the double standard is at least as relevant an issue in the field of information security as in the field of SE. One key objective of having the concept of maturity levels is to sketch "objective and universal" criteria, which is able to indicate the maturity of all kinds of organizations. By developing such criteria, the major objective is not to show the maturity level for the organization adopting the maturity criteria (inter-organizational) – although this is also a secondary objective of maturity standards - in which case the problem of the double standard is not so crucial. As with CMM, one crucial aim of setting up maturity criteria is to assist other organizations, third parties, business partners, etc to ensure that organizations which they deal with have certain level of information security. Recognizing this, it is justified to presume that the increasing recognition and use of a widely accepted maturity criteria would increase the incentives of organization to score high in terms of this IS security maturity criteria (cf. O'Connell & Saidian, 2000).

Spot focus. Bollinger & McGowan (1991 p. 33) levelled the criticism that the focus of maturity inspection is on prefixed spots, the result being that the criteria do not pay any attention to a holistic overall maturity posture. To illustrate this problem, Bollinger & McGowan submit the case where one person painting, say, a car does the job very well in certain spots leaving

other places without any paint (case A), scores equal high on the maturity scale as another person painting the whole car consistently well (case B); hence, the label spot focus. Clearly, the latter option (B) is more mature in terms of painting, but as the SW maturity criteria only examine certain spots, they lack the overall maturity estimation, and both (A and B) would scale equally high on the maturity scale, given that the measurement idea identical to SW maturity criterions is used (Bollinger & McGowan, 1991). Moreover, if such faults were a characteristic of security maturity criteria, it would result in organizations securing IS/SW possibly concentrating heavily only on certain places in order to increase their maturity level, whilst bestowing less or no attention on certain other aspects not covered by the maturity model (as in the case A in the aforementioned example).

Four categories *degrees of ambiguity* are proposed (Pfleeger et al., 1994): reference-only, subjective, partially objective and objective. Reference-only means a situation where the standard prescribes something which is does not provide any concrete means for ensuring compliance. For example, a prescription: "risk analysis should be carried out" without any indication of what the results of good risk analysis would be is an example of a reference-only practice. The problem is the lack of information concerning e.g. what good risk analysis practice should include and what is the scope of such risk analysis. The subjective situation is the case when the goodness/scope of a practice is left to be determined on the basis of an expert judgment. E.g. a prescription "risk analysis method needs to be applied with respect to relevant assets" is a case in point. Partially refers to a situation, which is more concrete than that of subjective practice, but still entailing some ambiguous information (e.g. "risk analysis needs to be accomplished with respect to relevant assets including"). Objective denotes prescriptions which give explicit guidelines with minimum inarticulateness. The advantage of the objective practice is the exactness it has compared to other alternatives. The weakness is that such general standards, as the objective one exemplifies, is difficult to build, and not wise in all cases (as organizations' business and security requirements/needs vary). The reference-only alternative is ranked as the worst alternative owing to the several important open questions it does not address. Proceeding towards the criterion of objectivity, it is suggested that organizations should build their specific standards.

3. ANALYSIS OF THE MATURITY APPROACHES

Operational focus

SSE-CMM does not pay close attention to this problem. At any rate, it does not trumpet the idea that evaluators should seek innovations. However, it does leave evaluators with some freedom to tailor some parts of process areas using their professional judgement. Yet, SSE-CMM says that one "*may tailor some aspects... to satisfy particularly needs*" (SSE-CMM, 1998). Unfortunately, it is not clear what this means exactly: what are some aspects? Or can one modify everything?

Information Security Program Maturity Grid. At the earlier level, the focus of this criterion is operational, as the following two examples from the second maturity stage illustrate. First: "*End-users view security restrictions as an unnecessary hindrance.*" (Stacey, 1996). Second: "The end-users' productivity is affected now both by the security incidents and by the safeguards set in place to protect the system." (Stacey, 1996). These examples indicate that organizations at the second stage do not stimulate security innovation; on the contrary, their security practice seems to debar normal practices. However, the fifth stage seems to pave way to innovations. Stacey (1996) requires that in order to qualify to the fifth stage, security people in organizations need to participate in research projects and "*its security professionals will be likely to achieve notoriety through presentation at ...conferences,... journals*". We see this citation implying that the fifth (the highest) stage imposes requirements for security innovations to be created by research/development processes selected results, of which, are reported to science through conferences and journals.

Murine-Carpenter maturity criterion. On the one hand, this criterion does not support the idea of innovations. First, it does not give direct hints in favour of innovations. Second, the milestones are based on a typical SW development life-cycle including the stages 'system security requirements', 'SW system security requirements', 'functional security architecture', 'modular security gating' and 'security testing' (Murine & Carpenter, 1984 p. 213). On the other hand, this criterion does not rule out the possibility of innovation; the use of innovations may become reality as this criterion gives a lot of freedom for developers to chose particular techniques/methods within each milestone (Murine & Carpenter, 1984 p. 213). However, the fact that the milestones are a must for all organizations, hinder the use of fundamental innovations that are not in synch with the milestone concept.

Naturalistic-mechanistic assumptions

SSE-CMM seems to contain ideas similar to those of behaviourism (a phenomenon can be quantified and controlled). For example, if A, then B, is an example of such a naturalistic-mechanistic causal law. SSE-CMM exhibits this idea, as the following citation illustrates: "*The SSE-CMM was developed with the anticipation that applying the concepts of statistical*

process control to security engineering will promote the development of secure systems and trusted products within anticipated limits of cost, schedule, and quality." (SSE-CMM, 1998). As seen in this citation, SSE-CMM takes Humbrey's analogy of manufacturing and SW development, along with the need of statistical control, seriously. The next citation supports this interpretation: "*Process capability is defined as the quantifiable range of expected results that can be achieved by following a process.*" (SSE-CMM, 1998). Also the fact that the fifth (highest) level is aimed at "*establishing quantitative goals...*" (SSE-CMM, 1998) indicates the role of the naturalistic-mechanistic view as it bears on SSE-CMM.

Information Security Program Maturity Grid. We do not find any naturalistic-mechanistic assumptions underlying this approach: it is not founded on observing industrial practices whilst trying to recognise cause-effect relations. This criterion does not state explicitly that the behaviour of users can be manipulated by cause-effect manner (such as whenever A, then B where e.g. A denotes "*awareness program accomplished*" and B "*users are motivated*"). However, it uses expression which one might regard imparting the flavour of a naturalistic-mechanistic assumption: "*because of the thorough security awareness training program, end-users are more vigilant and tend to initiate more incident reports.*" (Stacey, 1996). Even though Stacey in the citation above provides an ideal and simplistic picture of hoped results of awareness programs, we do not find his thinking couched in a naturalistic-mechanistic view.

Murine-Carpenter maturity criterion provides many hints of a naturalistic-mechanistic view. On the one hand, it repeatedly states the aim of laying down a quantifiable maturity criterion (Murine & Carpenter, 1984 p. 207, 208). On the other hand, it does not directly assert the existence of certain mechanistic-causal relationships. However, the fact that this criterion is concentrated on technical aspects only suggests that its worldview is very much of a naturalistic-mechanistic kind. The fact that the human component is not recognized or considered at all further supports our conclusion.

Stable versus emergent organization structures and functions

None of these maturity standards fully recognizes the issues which secure SW/IS development in emergent organizations pose. Some of the standards do better than others, and we shall analyze the each criterion in detail next.

SSE-CMM adopts highly stable IS security development approach. In fact, the way IS security development is contrived, pursuant to SSE-CMM, makes it perhaps the most rigid of the alternative maturity approaches. The whole maturity approach itself is close to one thousand pages long, the evaluation process is formal (and long) proceeding through all points and stages starting from the first stage. Moreover, the formulation and

functioning of the appraisal process is formal and includes bureaucratic elements. For example, there are several appraisal/appraised organizational roles that are recognized to be fulfilled in the evaluation process, such as appraisal facilitators, evidence custodian, voting members, observers (mentioned in appraisal organizations) and site coordinator, executives, executive spokesman, project leader and practitioner (mentioned in roles in the appraised organization). The SSE-CMM also recommends that the appraisal process to determine the maturity of an organization's security activities should take 1002 total working hours and ideally involve 30 people! To use 1002 hours just to evaluate the security level of an organization may be far too much, particularly for small emergent organizations. Yet, the appraisal process includes 18 phases and sub-phases; planning (3 sub-phases), preparation (4 sub-phases), on-site (7 sub-phases), and reporting (4 sub-phases). Things could be much worse from the point of view of emergent organizations. Fortunately, SSE-CMM gives the evaluators/target of evaluation freedom to choose the particular goals of the evaluations. Moreover, the assessment tool includes the concept of "tailorable parameters" allowing the evaluators e.g. to decide autonomously e.g. the scope of the evaluation with respect to these parameters.

Information Security Program Maturity Grid. Organizations scaling at the low level in terms of this maturity criterion are those not yet ready for emergent IS development. A few examples follow: "*Security is viewed as commodity that can be bought on the open market.*" This example from the second level indicates an assumption that general security solutions can be unearthed e.g. from standards. Here is another example from the second level: "*The officer will identify the significant threats and develop policies and procedures in response to the most frequently occurring crises.*" This implies that a stable environment is assumed for organizations belonging to the second level - they are waiting for "most frequently occurring crises". Yet, Stacey (1996) also recognizes the potential complications if organizations follow the pattern of stable organizations: "*Losses may be high especially when they do not follow the historical trend.*" In the third level, we see an increasing recognition of the idea of emergent organizations, as the following passage from the third level shows: "*security is no longer viewed solely as a commodity that can be purchased. Rather, information security must be designed consistent with an enterprise's needs-it must be designed from within.*" This is a first step towards the recognition that in an emergent organization security needs originate from the organization's mission, not from outside in the form of a generic security package. To give a second example: "*Previously prepared risk analysis become stale and demonstrate loose applicability to the evolving environment.*" The recognition of the inadequacy of the previous risk analysis in evolving an

environment in the latter citation also demonstrates a shift in thinking towards the idea of IS/SW development in emergent organizations.

The fourth level continues by giving support for the requirements posed by an evolving business environment. Two examples, from the fourth maturity level, follow. First, in order for an organization to be at the fourth level, it should: "*closely reflects the enterprise's environment and respond to the enterprise's evolving needs*". As a second example: "*Threats are continually re-evaluated based on the changing threat population and on security incidents.*" Both these examples clearly demonstrate a readiness on the part of fourth stage organizations in an era of emergent organizations. Finally, we see that the fifth stage supports the idea of emergent organizations as well. Consider the following citation: "*continual information security process improvements through research and participation and the sharing of knowledge in public and professional forums.*" This is an example of an ongoing analysis of a natural situation for emergent organizations (cf. Truex et al., 1999). On the negative side, Stacey's approach does not pay attention to the requirements arising from a fast pace of development in the case of emergent organizations.

Murine-Carpenter maturity criterion. Regarding the question of stable versus emergent organizations, this criterion lies somewhat between these two views. One the one hand, it suggests well-known aspects such as the five milestones. On the another hand, its prescriptions, such as milestones, lie at very high level of abstraction and leave the choice of particular techniques for the practitioners or users of the maturity criterion (Murine & Carpenter, 1984 p. 213). Yet, purely going through this criterion do not necessarily require a huge number manpower/working hours, as opposed to SSE-CMM, and generally it is not very rigid. Our conclusion is that the Murine-Carpenter maturity criterion may be of use to organizations which purely wish to improve their SW security in an emergent environment.

Double standard

As we understand it, no maturity standards explicitly address this issue. The Information Security Program Maturity Grid and the Murine-Carpenter maturity criterion does not come close to this issue at all. SSE-CMM comes closest to this issue, and therefore is the only one considered (see below).

SSE-CMM. The closest recognition of double standard is the following statement: "*Evidence must be weighed by the Appraisal team in that the source of the information is taken into consideration when the evidence is considered. For example, evidence from questionnaires or interviews may be considered less valid in that they are more prone to misuse or misunderstanding. Thus, the team might look for a certain amount of corroborating evidence from other sources, such as documents*" (SSE-

CMM, 1998b p. 80). Two things emerge from this citation. First, SSM-CMM does not provide any explicit guidance on recognizing and addressing the problem of the double standard, excepting evaluators' intuitions. Secondly, we understand this citation to imply that the evaluators are advised to pay more attention to quantified than qualitative evidence such as interviews (consider: "*may be considered less valid*"). However, the existence of quantified evidence *per se* cannot be regarded as meeting the case, since quantified data is also easy to fabricate and tamper with in an era of computers.

Spot focus

SSE-CMM. In case of SSM-CMM, on the one hand the process areas (and particular detailed questions within each process area) are the generic and predefined spots: "*while the PAs are generic, the Sponsor may tailor some aspects of PAs to satisfy particular needs*" (SSE-CMM, 1998). In that light, SSM-CMM succumbs to the fallacy of the spot focus. On the other hand, the organization can select the process areas to be included in the study. Yet, with respect to each process area there are a few "*tailorable parameters*", which organizations may modify. However, these two points do not remove the spot focus fallacy; the process areas and tailorable parameters are prefixed with the result that one cannot make one's own maturity spots. SSE-CMM also includes a hint, which might be interpreted as allowing refinement: "*although the SSAM* [the assessment method of SSE-CMM] *is a defined method, ...organizations may need to further refine particular aspects of the method to meet individual sponsor goals and expectations. All refinements must be documented and agreed upon by the sponsors and the appraisal organization.*" However, it is not clear whether this is constrained by tailorable parameters, or whether one can modify anything as long as the modifications are agreed upon.

Information Security Program Maturity Grid. In the fifth stage, the objectives are defined loosely with a result that Stacey's Information Security Program Maturity Grid eschews the fallacy of the spot focus.

Murine-Carpenter maturity criterion. As can be inferred from earlier discussions, in principle the Murine-Carpenter maturity criterion entails the spot focus fallacy. The five milestones and 11 security criteria are universal, i.e. they should be embedded in every mature secure SW development endeavor. However, the fact that milestones are only mandatory at a very abstract level whilst concrete methods/techniques to be used at low levels are non-mandatory, may decrease the problem of the spot focus.

Degrees of ambiguity

The degrees of ambiguity with respect to SSE-CMM range from reference only to objective. To some extent, degrees of ambiguity such as the subjective will suffice, and may even be necessary. Reference-only ambiguity is problematic, however. SSE-CMM resorts frequently to the use of reference-only practice. To give an example, we see the following point in Base Practice 1: "*manage security awareness, training, and education programs for all users and administrators*" (SSE-CMM, 1998), as an example of reference-only practice. SSE-CMM does not really indicate what such concepts as "awareness" or "management" mean. Does the term awareness refer to "being aware of something [security]", or to a state of affairs where employees are fully committed to security policy – the latter is not stated by SSE-CMM. It results from the reference-only practice that SSE-CMM does not provide any guidance on how one can know that employees are aware of – or committed to - security guidelines.

Information Security Program Maturity Grid. The degree of ambiguity of Stacey's (1996) information security program maturity approach entails both reference-only and subjective views. Imperatives such as organize a "*thorough information security training program for end-users*" are an example of a reference-only view. It does not imply what a good information security training program includes. We also found a subjective pattern "*users are empower and encouraged to evaluate and develop their own risk-based management strategies and to customize the enterprise's existing information security program to respond to they own needs*". This example provides clear guidance with respect to customization, given that end-users know their own needs, but it does not give any indications regarding the process of "risk-based management strategies", such as what a good process for accomplishing such risk-based management strategy might contain.

Murine-Carpenter maturity criterion. The Murine-Carpenter maturity criterion incorporates all degrees of ambiguity. On the negative side, the criterion utilizes a great deal of reference-only practice, therefore offering no practical help to developers. Sometimes the objective practice may be fallacious, as well, as indicated in the second section. For example, consider the fifth security-testing milestone: "System is tested for an illegal entry at all levels" (Murine-Carpenter, 1984 p. 213). This is objective practice at least insofar as the term "illegal" is concerned. However, security people may not want to prevent only "illegal" entry into a system, but rather unauthorized or unwanted entry.

4. DISCUSSION AND IMPLICATIONS OF THE FINDINGS

In spite of the fact that information security literature abounds in discussion of standards, the existing maturity criteria for securing IS/SW have largely been ignored. This paper analysed the existing maturity approaches for securing IS/SW. In addition to self-assessment, the maturity approaches are aimed at demonstrating to organizations and the public/third parties/customers confidence in the security level/maturity of an organization. In fact, it is the latter factor, which separates general information security management standards (mainly for inter-organizational self-assessment) from information security maturity management-oriented endeavours (inter-organizational self-assessment and public dimension assessment). Approaches under the banner of "evaluation standards" the Common Criterion being perhaps the most notable (Caplan & Sanders, 1999; Chokhani, 1992) are focused on technical aspects, computer systems and/or the very end of the development process or SW products (cf. Overbeek, 1995) with the result that they cannot be regarded as information security management-oriented maturity endeavours. For these reasons, such technical or computer-oriented standards are omitted from the present analysis.

Operational focus. Like CMM (cf. Rifkin, 2001), the maturity models – SSE-CMM and Murine-Carpenter maturity criterion - are anti-innovative. They tend to stress the use of the existing and workable practices for securing organizations' ISs. First, they do encourage neither creative and innovative thinking nor paradigm/research program changes, but rather uphold the use of existing practices. For this reason, we see that they are not good candidates for university education, which is perhaps the most important forum for achieving reform through education. Second, organizations which adopt innovation as their main competitive strategy gain nothing from the adaptation of these maturity criteria. Third, organizations using state-of-the art methods/techniques may perform badly in maturity estimations, since the old criteria do not recognize these new techniques. Stacey's Maturity Grid, in turn, can cope well with innovations. In fact, on the highest level, it requires the organization's security people to participate in research projects, thereby necessitating organizations to create innovations. On the final analysis, the Murine-Carpenter maturity criterion does not support the idea of innovations as the milestones are based on an existing well-known SW development life-cycle and, more importantly, they are universal. However, the fact that this criterion gives developers the freedom to chose the particular techniques/methods within each milestone (Murine & Carpenter, 1984 p. 213) therefore paving way to innovations, is a positive move towards the possibility of achieving security innovations.

Naturalistic-mechanistic. SSE-CMM seems to succumb to the fallacy of the naturalistic-mechanistic view. It strongly advocates a view according to which security phenomena should be quantified and controlled. In fact, the whole aim of this maturity criterion is to identify industrial practices where there is an effort to recognize cause-effect relations, and turn these into form of maturity standard. Whereas such approach might be adequate for pure computer systems having no social dimensions, it is inadequate for addressing information systems security, where there is a human or social component. Stacey's (1996) critetion does not make naturalistic-mechanistic assumptions. The Murine-Carpenter maturity criterion also is strongly coloured by naturalistic-mechanistic assumptions as it aims to sketch a quantifiable maturity criterion. Even though it does not explicitly argue in favour of casual relationships, its underlying worldview is naturalistic-mechanistic since e.g. users are not recognized by this criterion.

Stable versus emergent. SSE-CMM assumes a very stable environment. The overall process for securing IS/SW, or evaluation security maturity level of IS/SW, prescribed by SSE-CMM, is a formal and rather unbending one. The maturity criterion by Stacey (1996) is able to incorporate the requirement laid down for secure IS/SW development in emergent organizations with increasing success in the higher stages (3-6). The Murine-Carpenter maturity criterion does not provide a clear answer to this issue. It prescribes universal milestones which, even though these are in conflict with the idea of IS/SW development in emergent organizations, are only applicable at the very highest level of abstraction. At the lower levels of abstraction, developers are able to choose freely the techniques they prefer. Hence, it may suit organizations desirous only of improving their SW security without any social concerns in an emergent environment.

Double standard. We found no maturity standards that explicitly address this issue. SSE-CMM is the only one which can be interpreted to vaguely touching on this issue, but it does not provide any concrete guidance on this matter.

Spot focus. SSM-CMM: the process areas are the generic and predefined spots. Thus, SSM-CMM succumbs to the fallacy of the spot focus. However, an organization can select the process areas to be included in the evaluation, and it allows for modifiable parameters called "tailorable parameters". Alas, these two do not remove the spot focus fallacy; the process areas and tailorable parameters are prefixed with a result that one cannot create one's own spots. Stacey's method avoids the fallacy of the spot focus, particularly in the highest stage, owing to the fact that it requires organizations' security development to be in synch with organizational business requirements and the prescriptions are expressed at a very high level of abstraction. In theory, the Murine-Carpenter maturity criterion entails the spot focus fallacy: the

five milestones and 11 security criteria are universal, even though the methods/techniques to be used at the low levels are discretionary.

The degree of ambiguity. Of the four degrees of ambiguity, the most lamentable one is the reference-only view. SSE-CMM embodies a great deal of reference-only practice. The degree of ambiguity of Stacey's (1996) approach entails both reference-only and subjective views. The Murine-Carpenter maturity criterion includes all degrees of ambiguity. The criterion makes much use of reference-only practice thereby offering no practical help to developers, and also utilizes objective practice in a detrimental manner.

On the basis of results of this analysis, the following implications for future research and practice are recommended. Pfleeger et al. reported with respect to SE standards that their "*effectiveness has not been rigorously and scientifically demonstrate..we have too often relied on anecdote, gut feeling, the opinions of expert or even flawed research, rather than careful, rigorous* [research]" (Pfleeger et al. 1994 p. 71), and continue that "*even when scientific analysis and evaluation exist, our standards rarely reference them.*" (Pfleeger et al. 1994 p. 72). We see that this is also the reality in the realm of information security management maturity standards. At any rate, the findings of this study suggest that the security management maturity standards have not learned from the their cognate SE maturity standards. The main suggestion is that information security management-oriented maturity standards should be revised to address the issues considered here. Also, numerous empirical studies are needed to study the relevance and validity in reality the individual prescriptions for alternative maturity standards. At present such studies are a few and far between. Yet, we would like to see the inclusion in any information security maturity criterion of a complete reference list of related work, with respect to each of the processes areas, milestones (or whatever is they are called), from where the prescriptions originate. Currently, practitioners have no evidence on which to judge whether the prescriptions suggested by the security management-oriented maturity criteria really make sense. With respect to the innovation vs. operational focus, it is suggested that future information security maturity standards should consent to looking for innovative and novel ways of securing IS/SW. Future standards should avoid the naturalistic-mechanistic and the spot focus fallacies and include means for tackling the problem of double standard.

Nonetheless, we would be glad if the future maturity standards would emulate Stacey's method and allow organizations more freedom in choosing the process areas in maturity evaluations according to their own business requirements. It is suggested that evaluators – particularly in emergent organizations – take more liberties in modifying the evaluation process for their own purposes. One strategy for organizations would be the fabrication

of their own in-house evaluation criteria and practice, which would be less formal, more lightweight and pay particular attention to the most crucial aspects of the organization's IS security practice. Finally, with respect to degrees of ambiguity, forthcoming maturity criteria should on the one hand avoid reference-only practice; and on the other hand, use objective practice judiciously to avoid the problems discussed.

5. CONCLUSIONS

Information security management standards and checklists have received a lot of attention. However, little have been done to study the existing information security management-oriented maturity models. To fill this gap, this study analyzed the alternative information security management-oriented maturity criteria from the point of view of a framework mainly synthesized from the IS and SE literatures. Implications for research and practice were presented.

6. REFERENCES

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

Baskerville, R., Pries-Heje, J., (2001), Racing the E-Bomb: How the Internet Is Redefining Information Systems Development Methodology. In B. Fitzgerald *et al.* (eds): Realigning Research and Practice in IS development: The social and organizational perspective (pp. 49-68). New York: Kluwer.

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

Boehm, B., (2000), Unifying Software Engineering and Systems Engineering. IEEE Computer, pp. 114-116.

Bollinger, T.B. & McGowan, C., (1991), A critical look at software capability evaluations. IEEE Software, Vol. 8, no. 4 , July, pp. 25-41.

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

Chokhani, S., (1992), Trusted products evaluation. CACM. Vol. 35, Issue 7, pp. 64-76.

Curtis, B., (2000), The global pursuit of process maturity. Software, Vol. 17, No. 4, p. 76-78.

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.

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

Harré, R., (2000), Laws of nature. In W.H. Newton-Smith (ed): A Companion to the Philosophy of Science, Blackwell Publisher, Oxford, UK, pp. 213-224.

Hirschheim, R., (1985), Information systems epistemology: An historical perspective. In: Research methods in information systems. E. Mumford et al. (eds), Elsevier Science Publisher.

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

Murine, G.E. & Carpenter, C. L., (1984), Measuring Computer System Security Using Software Security Metrics. In Computer Security: A global challenge, J.H. Finch and E.G. Dougall (eds.). Elsevier Science Publisher.

O'Connell, E. & Saidian, H., (2000), Can you trust software capability evaluations? Computer, Vol. 33, Issue 2, pp. 28-35.

Overbeek, P.L., (1995), Common Criteria for IT Security Evaluation - Update Report. Proceedings of the 11th International Conference on Information Security (IFIP/SEC'95).

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.

Pfleeger, S.H. & Rombach, H.D., (1994), Measurement Based Process Improvement. IEEE Software, vol. 11, no. 4, Pp. 9-11.

Pfleeger, S.H., Fenton, N., & Page, S., (1994), Evaluating Software Engineering standards. IEEE Computer, Vol. 27, no. 9, pp. 71-79.

Pfleeger, S.H., (1999), Albert Einstein and Empirical Software Engineering. IEEE Computer, Vol. 32, no. 10, pp. 32-37.

Ray, C., (2000), Logical positivism. In W.H. Newton-Smith (eds): A Companion to the Philosophy of Science, Blackwell Publisher, Oxford, UK, pp. 243-256.

Rifkin, S., (2001), What makes measuring software so hard? Computer, May/June, p. 41-45.

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.

Siponen, M.T. & Baskerville, R., (2001), A New Paradigm For Adding Security Into IS Development Methods. Advances in information security management & small systems security. MA: Kluwer Academic Publishers.

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

Solms, R., (1997), Can Security Baseline replace Risk Analysis? Proceedings of the 13th International Conference on Information Security, 14-16 May, Copenhagen, Denmark.

Solms, R., (1998), Information security management: the Code of Practice for Information Security Management. Information Mgt & Computer Security. Vol. 6, no. 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.

SSE-CMM, (1998), http://www.sse-cmm.org.

Stacey, T.R., (1996), Information Security Program Maturity Grid. IS Security. Vol. 5, No.2.

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

Truex, D., Baskerville, R. & Travis, J. (2000), Amethodical Systems Development: The Deferred Meaning of Systems Development Methods. Accounting, Management and Information Technology, Vol. 10, pp. 53-79.

Voas, J., (1999), Software quality's eight greatest myths. Software, vol. 16, no. 5, p. 118-120.