Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2009 Proceedings | Mediterranean Conference on Information Systems (MCIS)

2009

Aligning Security Awareness With Information Systems Security Management

Aggeliki Tsohou
Dept. of Information and Communication Systems Engineering, University of the Aegean, agt@aegean.gr

Maria Karyda
Dept. of Information and Communication Systems Engineering, University of the Aegean, mka@aegean.gr

Spyros Kokolakis
Dept. of Information and Communication Systems Engineering, University of the Aegean, sak@aegean.gr

Evangelos Kiountouzis
Department of Informatics, Athens University of Economics and Business, eak@aueb.gr

Follow this and additional works at: http://aisel.aisnet.org/mcis2009

Recommended Citation
Tsohou, Aggeliki; Karyda, Maria; Kokolakis, Spyros; and Kiountouzis, Evangelos, "Aligning Security Awareness With Information Systems Security Management" (2009). *MCIS 2009 Proceedings*. 73.
http://aisel.aisnet.org/mcis2009/73

This material is brought to you by the Mediterranean Conference on Information Systems (MCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

ALIGNING SECURITY AWARENESS WITH INFORMATION SYSTEMS SECURITY MANAGEMENT

Tsohou, Aggeliki, Dept. of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece, agt@ aegean.gr
Karyda, Maria, Dept. of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece, mka@ aegean.gr
Kokolakis, Spyros, Dept. of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece, sak@aegean.gr
Kiountouzis, Evangelos, Department of Informatics, Athens University of Economics and Business, Athens, Greece, eak@aueb.gr

Abstract

This paper explores the way information security awareness connects to the overall information security management framework it serves. To date, the formulation of security awareness initiatives has tended to ignore the important relationship with the overall security management context, and vice versa. In this paper we show that the two processes can be aligned so as to ensure that awareness activities serve the security management strategy and that security management exploits the benefits of an effective awareness effort. To do so, we analyze the processes of security awareness and security management using a process analysis framework and we explore their interactions. The identification of these interactions results in making us able to place awareness in a security management framework instead of viewing it as an isolated security mechanism.

Keywords: *Security Management, Security Awareness, Process Analysis*

1 INTRODUCTION

Information systems security management comprises understanding information security requirements, establishing security policy and objectives for information security, implementing and operating controls to manage information security risks, monitoring and reviewing the performance and effectiveness of them and continuous improving (*ISO/IEC 27001, 2005*). Security awareness is a critical element of security management (*CSI, 2008*), that refers to the process of making users aware of security risks, focus their attention on security and allow them to recognize security concerns and respond accordingly (*NIST, 2003*). Security awareness has been studied by security researchers and practitioners mainly as a risk mitigation mechanism, separately from other information security management processes. As a result, it is not clear how the process of information security awareness interacts with other security management practices. In this paper we aim at exploring the research question "*in what ways is awareness connected to the other processes of security management and what are their interactions?"*. Investigating this question is important, since revealing the interactions of the two processes influences security practitioners with regard to time and resource allocation, the time-plan and the overall security project-management. In addition, it will be of use to security researchers, as it will enhance exploring the problematical issues of security awareness in the security framework where they happen. For this purpose, we first define organizational processes and then we use this framework to define the two processes and their interaction. Our analysis does not aim at identifying a process modeling technique, but a framework of conceiving organizational processes in order to make sense of the awareness and security management interaction.

The paper is organized in five sections. In the next section we describe current approaches for defining organizational processes. Section 3 is dedicated in identifying the ways researchers regard the interaction between awareness and security management. In Sections 4 and 5 we analyze security

management and awareness, accordingly, using the GED framework to gain insight into the process goals, activities or problems. The following section presents a discussion concerning the interactions between awareness and security management that have been identified. Finally, the conclusions and further research issues are presented.

2 DESCRIBING ORGANIZATIONAL PROCESSES

An organizational process can be defined as "*a set of logically-related tasks performed to achieve a defined organizational outcome*" (*Davenport and Short, 1990*). *Crowston (2000)* differentiates two basic perspectives in defining organizational processes:

I. Goal-oriented, which includes the identification of the final process result, the parameters that have to be fulfilled for the goal's achievement, the transformation of input to output for its accomplishment, the recipient of the process result as well as the person that poses the process goal or the person who benefits from it, and

II. Sequence-oriented, which defines a sequential and hierarchical recording of all involved events. This includes identifying a set of observations about the events that happened in past performances of the process and a set of predictions about what will happen in future performances.

A complementary perspective to the sequence-oriented approach views organizational processes as a construct of events, whose realization is bounded by a set of *restrains and interdependences*. As, *Crowston (2000)* refers *Malone and Crowston (1994)* proposed two major classes of dependencies: a) flow or producer/consumer dependencies and b) shared resource dependencies. The first class arises when the product of an activity is a prerequisite for the execution of another activity. The second class of dependencies arises when two or more activities require the same resources. *Davenport and Short (1990)* classify organizational processes into three major dimensions according to: 1) the organizational entities or subunits involved (interorganizational, interfunctional or interindividual processes), 2) the type of objects manipulated (physical or informational), and 3) the type of activities taking place (operational or managerial).

In this paper, we follow the approach proposed by *Katzenstein and Lerch (2000)* for modeling organizational processes, which incorporates all the above mentioned elements of organizational processes: goals, sequence and dependencies and is referred to as the GED (Goal – Exception – Dependency) framework. Besides these, GED also takes into account elements of possible deviations from the expected process development. In this approach, an organizational process comprises the following elements:

a. **Goals** of either the overall process or of individuals participating in the process.

b. **Roles**, which present a linked set of actions, obligations, perspectives, and other concerns which characterize an individual or group of individuals.

c. **Exceptions**, which are reasons of deviations from standard development of the process, such as random occurrences, errors, conflicting organizational or political goals.

d. **Dependencies,** that include dependencies from logistic, financial, informational, or managerial elements which occur within the establishment of relationships among the process members to achieve their goals.

This approach provides an analytical tool for making sense of organizational processes in a high level of abstraction. Moreover, the GED framework has been validated according to a set of process representation criteria (*Katzenstein and Lerch, 2000)* so as to a) capture what goes on in the process (content criterion), b) capture what may emerge or change in the process (status criterion), and c) provide practical and user friendly representations (presentation and use criterion). During our analysis we have identified a number of exceptional deviations or dependency situations, which could not be

categorized under the predefined exceptions or dependencies. An example refers to conflicting perceptions that may result in unpredicted process developments. For this reason we have enriched the GED framework to include additional dependencies and exceptions' categories: perceptions, availabilities and trust have helped us capture more social aspects of the processes that constitute dependencies and exceptions.

3 CURRENT PERSPECTIVES ON THE INTERPLAY BETWEEN AWARENESS AND SECURITY MANAGEMENT

Information security awareness can be considered as an internal element of information security management, but up to now, it has not been thoroughly studied in relation to its organizational and security management context. In the following, we identify the ways researchers perceive the association of awareness and security management within the body of security literature, using the basic criteria of process representation (goal-orientation, sequence-orientation, restrains and dependencies) described earlier.

Many researchers discuss the interaction between the two processes in terms of sequence. *Hansche (2001)* and *Everett (2006)* place awareness after the security management tasks of risk analysis, security policy formulation and countermeasures specification have been fulfilled. *Okenyi & Owens (2007)* claim that establishing a security policy is a prerequisite towards building a security awareness program. *Peltier (2005)* argues that organizational goals are the core of security management and, thus, all security management activities should be centered on business goals. Under this perspective, the author views security awareness connected to security management in a goal-oriented way: awareness is connected through the established business goals into a coherent security management framework and the role of awareness is to support the business goals and to make the security program acceptable by the members of the organization. For example, within the process of awareness the reasons for adopting a security policy should be justified in terms of the business goals it would serve. Interactions between awareness and security management can be clearly identified in *Spurling's (1995)* empirical research. The author proposes a security program development that sequentially connects awareness with other security management activities. Awareness is placed in the phase of risk treatment, after security measures and policies have been specified. Spurling also connects awareness to security management, in terms of goals, as it is reported that security awareness should be aligned with the security vision and philosophy.

Power and Forte (2006) establish a more concrete connection between awareness and security management in their case study: awareness and security management goals both serve the overall security mission. In addition, the organization establishes a global security team which is responsible for security management and awareness at the same time. *Vroom and von Solms (2002)* claim that formulating a security policy constitutes a prerequisite for designing the process of security awareness, since the former defines the tasks for the personnel, the procedures for reporting security incidents and for educating staff. Thus, the processes of security policy formulation and awareness are dependent (information and managerial dependency). Financial and managerial dependencies are widely accepted by most researchers (*Everett, 2006; Okenyi and Owens, 2007; Peltier, 2005; Power and Forte, 2006*) as management commitment to awareness and cost approval are considered essential.

According to the approach adopted by *ISO/IEC 27001 (2005*), security management unfolds in four stages, namely: a) Plan, b) Do, c) Check, and d) Act whilst the process of awareness is placed, in a sequence-oriented manner, within the second stage of security management (in the 'Do' phase) (p. 6, 30), as depicted in Figure 1. *ISO/IEC 27002:2005* is closely interrelated to *ISO/IEC 27001:2005*, and provides implementation guidance for designing controls. It proposes control objectives and controls, structured in a categorization of eleven clauses that aim at meeting the requirements identified by a risk assessment process. The *ISO/IEC 27002:2005* best practices mainly refer to the 'Plan' and 'Do' phases. *ISO/IEC 27002:2005* places awareness in several clauses, namely: security policy (awareness requirements

should be defined in the security policy document), organization of information security (as a part of management's commitment to security and as a way of achieving internal security co-ordination among managers, users, administrators, application designers, etc.), human resources management (during employment a level of awareness relevant to the employees' roles and responsibilities within the organization should be aimed regarding the security procedures and policies, and the correct use of information processing facilities before access is granted), information security incident management (awareness should include information on known threats, who to contact for further security advice and the proper channels for reporting information security incidents, business continuity management (awareness should create understanding of the business continuity processes), communications and operations management (awareness should be a control for the protection of malicious code), and compliance (awareness should promote the intellectual property rights protection and data protection principles).

Conclusively, as indicated by relevant literature, the processes of security management and awareness are not independent from each other but are interconnected; however their boundaries remain unclear to security researchers and practitioners.

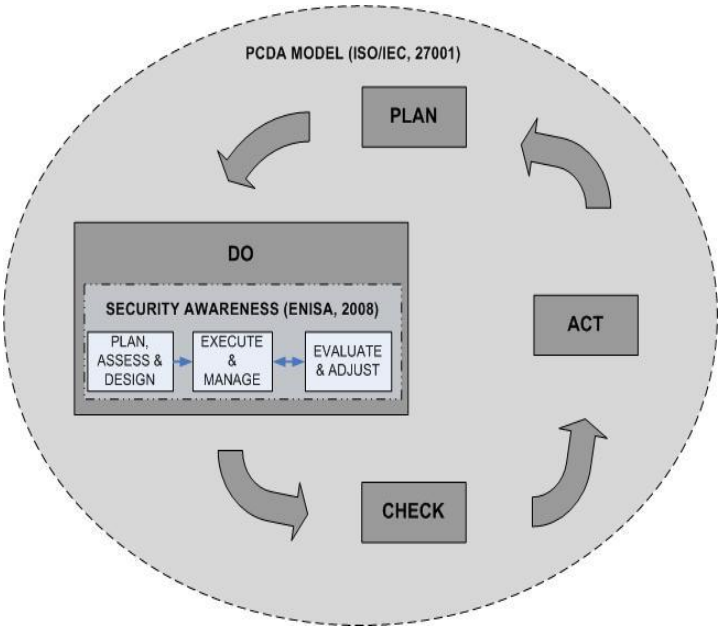

Figure 1: Awareness and security management interaction (ISO/IEC 27001, 2005; ENISA, 2008)

4 ANALYZING THE PROCESS OF INFORMATION SECURITY MANAGEMENT

In order to further understand the interplay between the processes of security management and awareness, we analyze the two processes using the GED framework, by identifying a) their goals, b) the roles that participate, c) the dependencies, and d) the exceptions that exist.

To begin with, according to the classification scheme proposed by *Davenport and Short (1990)* security management is a horizontal process that crosses different divisional units or departments of organizations; thus it is an *interfunctional* process (*Davenport and Short, 1990)*. Both *physical and informational* objects are manipulated within security management, where physical objects include the physical infrastructure of security measures while informational objects include security plans, policies etc. Typical activities of security management are mainly *managerial*, since they support and control the operational tasks; such as, for example, the authentication and auditing tasks that aim at constraining and controlling personnel while performing their operational duties.

In the following, we base our analysis of the process of security management provided in the widely accepted security standards *ISO/IEC 27001 (2005)* and *NIST (2002*). Since it is not our aim to model the

process of security management, but to make sense of its main components, this identification is not meant to be exhaustive but exploratory.

According to *ISO/IEC 27001 (2005),* the fundamental security management goals are preserving integrity, availability and confidentiality of information. *NIST (2002)* adds accountability, and also authenticity, non-repudiation and reliability as complementary security management goals (*ISO/IEC 27001, 2005*). Security management involved roles include decision makers, operation staff, users and developers (*ISO/IEC 27005, 2008*).

4.1 GED analysis of security management 'Plan' phase

The planning phase of security management (*ISO/IEC 27001, 2005*), or as is also known the phase of establishing the Information Security Management System (ISMS), includes defining the ISMS policy, as well as the objectives, processes and procedures which are relevant to managing the risks and improving information security in order to deliver results in accordance with an organization's overall policies and objectives.

The goals of this phase are to define the scope and boundaries of the ISMS, to identify a risk assessment methodology that is suited to the ISMS, to establish a security team that will plan and operate the ISMS, to develop criteria for accepting risks and identify the acceptable levels of risk, to perform risk assessment, to evaluate potential mitigating strategies, to select countermeasures for the treatment of risks, to define an ISMS policy, and to obtain management approval of the proposed residual risks and management authorization to implement and operate the ISMS. It should be noticed that within the formulation of the risk treatment plan, *ISO/IEC 27002 (2005)* proposes the introduction of awareness activities to achieve several control objectives (clauses of security policy, organization of information security, human resources security, communications and operations management, information security incident management, business continuity management, and compliance).

In addition to the exception and dependency types proposed by GED, we have also identified the influence of intangible dependencies (such as trust and perceptions), unavailability and deliberate actions exceptions. Overall, the following dependencies have been identified:

- Informational: These include architectural and functional requirements, interfaces, data, threat and vulnerability evaluations which are required for performing risk assessment.
- Management approvals: for risk management, investments, involving personnel.
- Trust: during communication of confidential information to the security team, especially when security management is outsourced.
- Resources: security management funding.
- Perceptions: Language and understanding between the involved parties.

Finally, the following exceptions may arise:

- Random events, such as advancements in technology and security, unclear system functionality and security incidents that raise attention to specific threats.
- Errors: Overrated or underestimated threats or impacts, missing software or hardware components.
- Conflicts: Different security perceptions, different security goals, opposing risk analysis evaluations, opposing risk mitigating strategies.
- Availability: Difficulties in meeting management, in arranging evaluation meetings.

4.2 GED analysis of the security management 'Do' phase

The second stage of security management (the 'Do' phase), entails the implementation of the ISMS policy, and the application of security controls, processes and procedures. Its goals are to formulate a

risk mitigation plan, to implement the selected controls, to define a measurement plan for the effectiveness of the selected controls, to implement training and awareness programs, to manage the operation and resources of the ISMS, and to implement incident and reporting procedures. We should notice that the implementation of the risk mitigation plan includes the implementation of the awareness activities that aim at the security policy, organization of information security, human resources security, communications and operations management, information security incident management, business continuity management, and compliance control objectives (*ISO/IEC 27002, 2005).* The dependencies we have identified are the following:

- Informational: they include the available security tools and techniques, organizational policies and software development methodologies.
- Resources: security measures implementation cost, training and education of security officers and other members.

The following exceptions may appear:

- Errors: user, operator or administrator errors that can lead to security violations, non-reporting of security incidents or vulnerabilities.
- Conflicts: following security guidelines may slow down system functionality and usability, users often ignore security practices.
- Perceptions: stakeholders do not understand their personal role in security.

4.3 GED analysis of the security management 'Check' phase

'Check' refers to assessing and measuring the process performance against the ISMS policy, measuring the objectives and practical experience and reporting the results to management for review. The goals of this phase are to execute monitoring and reviewing actions for detecting errors, identifying and handling of security breaches and preventing security incidents, to undertake regular reviews of the effectiveness of the ISMS, to measure the effectiveness of controls, and to review risk assessments at planned intervals.

The identified dependencies are:

- Informational: reports from event and audit tools, security metrics.
- Trust related: stakeholders should feel trust to report a security violation or vulnerability.

Furthermore, the following exceptions may appear:

- Random events: for instance, no identification of vulnerabilities during sample inspections.
- Errors: such as the underestimation of a security incidence by users.
- Deliberate actions: deliberate modification of event or audit trails, hiding of evidence.
- Conflicts: deviations on the strategies to handle a security incident.
- Availability: of the security officer to respond to users' security doubts.

4.4 GED analysis of the security management 'Act' phase

The final phase of security management is the Act phase, where corrective and preventive actions take place guided by the internal ISMS audit and management reviews, in order to achieve continual improvement of the ISMS. Its goals are to implement the identified improvements, to take appropriate corrective and preventive actions, to communicate the actions and improvements to all interested parties and agree on how to proceed, and to ensure that planned improvements achieve their intended objectives.

For the Act phase the identified dependencies are:

- Informational: the previous stage (checking) reports and results.
- Availability: of the security team to realize adjustments.
- Management approvals: to conduct new security study or to implement changes.
- Resources: funding of changes.

Finally, the following exceptions may occur:

- Errors: changes can lead to system dysfunction.
- Conflicts: with regard to the selection of adjusting actions.

5 ANALYZING THE PROCESS OF SECURITY AWARENESS

With regard to the classification proposed by *Davenport and Short (1990)*, awareness is an *interfunctional* process that crosses different divisional units or departments of organizations; e.g. the Human Resources department for identifying and dividing audience groups and the Technical Department for exploring major users' errors and problems. The object types are mainly *informational,* such as the awareness work plan, security messages, or feedback questionnaires. Physical objects may also be included, for example posters, leaflets or other artifacts that convey security messages. Finally, typical awareness activities are *managerial*; they support and inspire the operational tasks; for example, they promote work practices that enhance the security vision. In the following we analyze the process of security awareness using the GED framework, by identifying the a) goals, b) roles, c) dependencies, and d) exceptions commonly found in awareness activities.

Major objectives of security awareness include a) changing users' behavior (*NIST, 2003*), b) changing users' work habits (*Hansche (2001*), and c) making users understand their personal role and responsibilities towards security (*Peltier, 2005*). The involved roles are not clearly specified; top management, managers, security officers may be involved in different cases. The activities of awareness unfold in three phases: a) Plan, Assess & Design, b) Execute & Manage, and c) Evaluate & Adjust (*ENISA, 2008*). *NIST (2003*) similarly describes the awareness and training lifecycle as comprising four steps: 1) program design, 2) material development, 3) program implementation, and 4) post-implementation.

5.1 GED analysis of the 'Plan, Assess & Design' phase

The 'Plan, Assess & Design' phase involves (*ENISA, 2008*) identifying needs, developing an awareness plan and establishing priorities. The goals of the first awareness phase are to establish the awareness team, to ensure a change management approach, to define awareness goals and objectives, to identify audience groups, to select awareness material, to develop a detailed work plan, to select communication channels and strategies, and to define indicators to measure the success of the program. This phase includes the activities of program design and material development of the *NIST (2003)* framework. Although the activities described are similar to *ENISA (2008*), the *NIST (2003)* standard pays additional focus on the selection of a centralized or distributed (to the organizational units) implementation. Taking into account the steps required to fulfill these goals, the following dependencies exist:

- Informational: information that is required for understanding the environment and setting the priorities, such as system architecture, functionality, users, organization policies, security policy, risk analysis results, system inventory and application user ID databases to determine all who have access.
- Management approvals: they are necessary for the conduction of the awareness program and the formation of the awareness team
- Resources: program funding, available communication channels, potential material.

At the same time, the following exceptions may intervene to the planning phase:

- Random events: confusing or conflicting system functionalities that makes audience groups segregation difficult.
- Errors: for instance, overloading awareness content with unnecessary information.
- Conflicts: different security perceptions or goals, different opinions about scheduling awareness actions or selecting centralized or decentralized implementation.
- Availability: difficulties in managing meetings or in arranging team meetings.

5.2 GED analysis of the 'Execute & Manage' phase

The 'Execute & Manage' step refers to all activities necessary to implement an information security awareness program (*ENISA, 2008*). This phase corresponds to the implementation step of the *NIST (2003)* framework. According to both standards, for this process to be executed and managed a needs assessment should have been conducted, a strategy developed, an awareness program plan for implementing that strategy should have been completed and material should have been developed. Its goals are to confirm the awareness team, to review the work plan, to implement designed actions, to deliver communications, and to document experience. Dependencies of the 'Execute & Manage' sub-process are:

- Informational: the documentation and results produced in the first phase, including audience group lists, communication channels, appropriate content, time-plan etc.
- Resources: funding awareness material (e.g. posters, leaflets).
- Availability: employees working hours for attending the program.

For this phase the exceptions that may happen include:

- Random events: emergent working events may prohibit employees' attendance.
- Errors: neglecting to write down important events during program conduction.
- Conflicts: managers that do not disengage their associates.
- Perceptions: language/terminology of security experts, difficulties in the understanding of the program by the users.

5.3 GED analysis of the 'Evaluate & Adjust' phase

The 'Evaluate & Adjust' phase (*ENISA, 2008*) includes procedures of formal evaluation and feedback mechanisms to evaluate the achievement of objectives initially established for the program and corresponds to the post - implementation step of the *NIST (2003)*. Its goals include evaluation of the effectiveness of the program, to review the feedback captured, to adjust the program and to re-launch the program (when it is necessary). The continuous monitoring could also be performed by an automated tracking system (*NIST, 2003*) that could capture key information regarding awareness and training program activities. For this phase the identified dependencies are:

- Informational: The goals that have been documented in the first phase, awareness metrics or indicators documented in the first phase as well etc.
- Resources: funding adjustments or new program execution.
- Management approvals: for adjusting the program or for new execution.

Finally, the exceptions that may happen are:

- Errors: Neglecting to take into account important events during evaluation.
- Conflicts: Opposing opinions regarding corrective actions.

6 DISCUSSION

As mentioned in section 3, awareness is typically perceived as a part of the implementation activities of security management. In this section we argue that there is an extended interplay between the two processes and that awareness activities interact with security management activities during all its stages.

The main implication of the traditional view, that is placing awareness within the 'Do' phase of security management cycle, is that awareness activities focus mainly on facilitating the application of the countermeasures, as revealed earlier in this paper. However, it has been suggested that security awareness objectives should not be narrowed in this way, but should also include goals such as the motivation of information system stakeholders. *Drevin et al. (2007*) identify the following fundamental awareness objectives: maximizing integrity, confidentiality and availability of data and hardware and maximizing acceptance of responsibility of actions. Therefore, the goal-oriented connection of awareness to the process of security management is wider than just enhancing the application of safeguards. In addition, we argue that security awareness can facilitate tackling security management dependencies and prevent its exceptions.

In the 'Plan' phase of security management a security team is defined, the organizational context is studied and the boundaries of the information system are specified. Awareness actions that could take place at the same time are the appointment of a security awareness officer or team and the study of organizational context and members to identify audience groups and communications channels. For example, during the security management 'Plan' phase users' security needs are examined for risk analysis purposes; an action that is also required for awareness 'Plan, Assess & Design' phase. In addition, *ISO/IEC 27002 (2005)* suggests the specification of security education, training and awareness requirements as a part of the security policy principles' formulation; such an activity is closely interconnected with the activities of awareness 'Plan, Assess & Design'. Moreover, security management planning could be hindered by conflicts regarding security goals. Awareness actions could confront this exception, since awareness aims at creating a common understanding of security by defining the main security concepts. This action, as *Furnell et al. (2007)* claim, would facilitate the creation of common security perceptions. In addition, during the 'Plan, Assess & Design' stage of the process of security awareness the available communication channels are examined and evaluated. The result of this activity could assist in confronting security management availability exceptions. Moreover, the creation of a common security perception among members of the security team would prevent conflicts and errors during risk analysis, since the threat, vulnerability and impact evaluations would be more informed and accurate. Finally, informing the security team with the results of recent research, surveys, statistical evidence and advancements in security technology would facilitate overcoming informational dependencies in security management planning.

Within the implementation phase of security management the interaction between the two processes is well established. Awareness activities facilitate the adoption of security policy and security practices by preventing the exceptions of perceptions, conflicts and also errors. This is achieved through raising the attention towards the importance of security, the personal role on security of the organizational members and also the importance of reporting security violations and incidents. Moreover, awareness activities are connected to the pursuit of several security control objectives as pointed out in *ISO/IEC 27002 (2005*), e.g. to ensure information security events and weaknesses are communicated in a way allowing timely corrective action to be taken (information security incident management clause).

During the 'Check' phase of security management, errors can happen if users don't report in time security incidents or vulnerabilities. Awareness is quite important in eliciting the sense of incident reporting to the users. Moreover, awareness actions could facilitate surmounting informational dependencies faced by administrators (e.g. provision of audit & event logging analysis criteria). Furthermore, making top management aware of the importance of keeping security management current could facilitate overcoming approval dependencies of the 'Adjusting' phase.

Overall, there are several informational dependencies posed to awareness activities that result from the process of security management. The security requirements identified during risk analysis feed the awareness content design or direct the focus on specific threats and vulnerabilities. Countermeasures and policies also provide input for the process of awareness; for example role-based access control would specify information regarding users' roles, rights and obligations or the communication channels to security officer in case of an incident. Therefore, the interconnections of security management and awareness are not narrowed to a single phase of security management, but instead awareness activities interact with security management activities throughout the entire process. Thus, the interplay between security management and awareness can be depicted as shown in Figure 2.

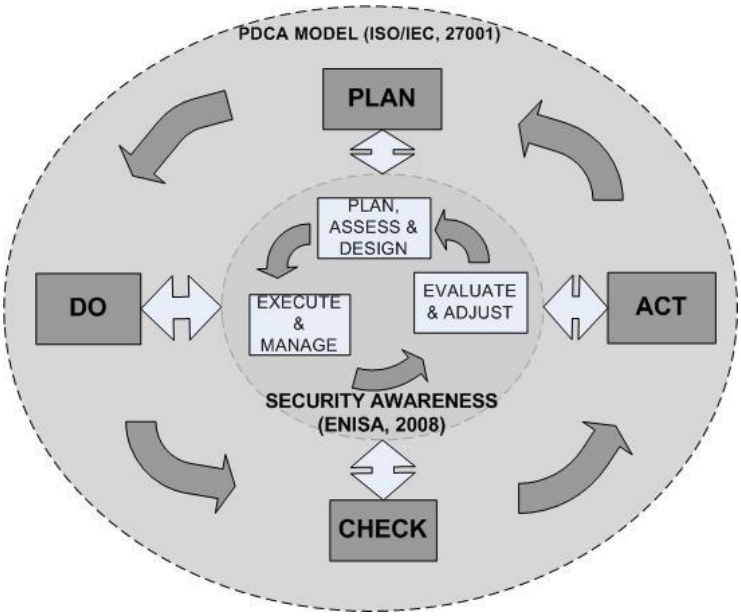

Figure 2: Extended interaction of security management and awareness

7 CONCLUSIONS AND FURTHER RESEARCH

This paper explores the way security awareness connects to the overall information security management framework. Up to now, awareness has not been studied in relation to other security management activities. Our analysis links awareness activities with security management tasks in terms of goals, events, people involved and interdependencies.

We have analyzed the processes of security management and awareness process separately and we have identified interactions between their goals, roles, dependencies or emergent events. Through the analysis we have come to the conclusion that security awareness should not be viewed as a collection of tasks narrowed to a single phase of security management (Figure 1), but as a process that should evolve in parallel to other security management activities (Figure 2). If designed and executed in this way (an indicative alignment of the two processes is presented in Table 1), the awareness process could facilitate security planning, the implementation of controls, security checking and adjusting by serving several goals simultaneously: compose a security awareness team that cooperates with the security team, facilitate the dialogue between the security experts and stakeholders involved, impede conflicts that come from ignorance or disinterest, provide information where informational dependencies exist and promote security policy adoption. Moreover, such an alignment would ensure that awareness actions also facilitate tackling security management dependencies and prevent its exceptions.

Another conclusion that stems from the analysis presented is that in both cases, it is hard to relate process goals with the individuals that pursue them or that are served by their fulfillment. Such a correlation would be beneficial for each process analysis individually but also for the examination of security management and awareness interactions. A further step would be to exploit the findings of the

analysis presented in this paper in order to formulate security management and awareness strategies in a way that acknowledges their interactions and practically implement these strategies in a real organizational setting. Furthermore, since awareness is only the first step of a security learning continuum (*NIST, 2003*) that proceeds with training and education, it would be of interest to adapt the process-oriented framework used in this paper studying training and education activities' interplay with security management tasks. Furthermore, similar analysis could be made based on other security standards describing the overall security management process, such as *NIST (2006*).

Security Management		Security Awareness	
PLAN	**Activities**	**Activities**	Plan, Assess & Design
	Establishment of a security team.	Determination of a security awareness officer or team.	
	Study of organizational context.	Study of organizational context.	
	Users' security needs are examined.	Organizational members are examined to identify audience groups.	
	Risk Analysis.	Communications channels are examined.	
	Specification of security education, training and awareness requirements	Creating a common understanding of security by defining the main security concepts.	
	Dependencies or exceptions	**Dependencies or exceptions**	
	Availability exceptions	Users' security needs and awareness requirements are required.	
	Conflicts regarding security goals	Risk analysis feed the awareness content design or the focus on specific threats and vulnerabilities.	
	Errors by overrated or underestimated threats or impacts.	Informational needs regarding program's content.	
DO	**Activities**	**Activities**	Execute & Manage
	Implementation of resulting countermeasures and policies.		
	Dependencies or exceptions		
	Following security guidelines slows down system functionality and usability, users ignore security practices.	Raising the attention towards the importance of security	
	Stakeholders do not understand their personal role in security.	Informing about the personal role on security of the organizational members	
	User, operator or administrator errors that lead to security violations, non-reporting of security incidents or vulnerabilities.	Informing about the importance of reporting security violations and incidence	
CHECK	**Activities**	**Activities**	
	Prompt identification of attempted and successful security breaches and incidents.	Eliciting the sense of incident reporting to the users.	
	Conduction of internal ISMS audits at planned intervals	Communication of audit & event logging analysis criteria	
	Dependencies or exceptions	The program will provide an incidence reporting structure; thus communication channels to the security officer would be identified.	
	Errors due to underestimation of a security incidence by users.	During the program the users would be informed about the communication channels available for private incidence reporting	
	Availability dependencies of the responding of security officer to users' security doubts.		
	Dependency on the establishment of trust for the stakeholders to report a security violation or vulnerability.		
ACT	**Activities**	**Activities**	Evaluate & Adjust
	Take appropriate corrective and preventive actions	Making top management aware of the importance of keeping security management current could facilitate approvals.	
	Communicate the actions and improvements to all interested parties		
	Dependencies or exceptions		
	Management approval to conduct new security study or to implement changes		

Table 20: The security management and awareness indicative alignment

References

Crowston, K. (2000). Process as theory in information systems research. Proc. of the IFIP WG 8.2 Intern. Conf.: The Social and Organizational Perspective on Research and Practice in Information Technology, Aalborg, Denmark.

CSI (2008). CSI Computer Crime and Security Survey2008, Robert Richardson. Retrieved from: i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

Davenport, T. & Short, J., (1990). The New Industrial Engineering: Information Technology and Business Process Redesign, In: Sloan Management Review, Summer 1990, 11-27.

Drevin, L., Kruger, H.A., & Steyn T. (2007). Value-focused assessment of ICT security awareness in an academic environment. Computers & Security, 26 (1), 36-43.

ENISA (2008). A new Users' Guide: How to Raise Information Security Awareness 2008. European Network and Information Security Agency. Retrieved from: http://www.enisa.europa.eu/doc/pdf/deliverables/new_ar_users_guide.pdf

Everett, C. (2006). Security Awareness: switch to a better program. Network Security, 2006 (2), 15-18.

Furnell, S.M., Bryant, P., & Phippen, A.D. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26, (5), 410-417.

Hansche, S. (2001). Designing a Security Awareness Program (I). Information. Systems Security, 9(6), 14-23.

ISO/IEC 27001 (2005). Information technology - Security techniques – Information security management systems - requirements. International Standards Association.

ISO/IEC 27002 (2005). Information technology -- Security techniques -- Code of practice for information security management. International Standards Association.

ISO/IEC 27005 (2008). Information technology — Security techniques — Information security risk management. International Standards Association.

Katzenstein, G., & Lerch, F. (2000). Beneath the surface of organizational processes: a social representation framework for business process redesign. ACM Transactions on Information Systems, 18 (4), 383-422.

Malone, T. W. & Crowston, K. (1994). The interdisciplinary study of coordination. Computing Surveys, 26 (1), 87–119.

NIST Special Publication 800-100 (2006). Information Security Handbook: A Guide for Managers, National Institute of Standards and Technology. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

NIST Special Publication 800-30 (2002), Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST Special Publication 800-50 (2003). Building an Information Technology Security Awareness and Training Program, National Institute of Standards and Technology. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Okenyi, P. O., & Owens, T. J. (2007). On the Anatomy of Human Hacking. Information Systems Security, 16 (6), 302-314.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. Information Systems Security, 14 (2),37- 48.

Power, R., & Forte, D. (2006). Case Study: a bold new approach to awareness and education, and how it met an ignoble fate. Computer Fraud & Security, 2006 (5), 7-10.

Spurling, P. (1995). Promoting security awareness and commitment. Information Management and Computer Security, 3(2), 20-26.

Vroom, C. & von Solms, R. (2002). A Practical Approach to Information Security Awareness in the Organization. Procs of the IFIP TC11 17th Intern. Conf. on Information Security: Visions and Perspectives, Cairo, Egypt.