A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations

Reza Alavi[1], Shareeful Islam[1], and Haralambos Mouratidis[2]

[1] The University of East London, United Kingdom
[2] University of Brighton, United Kingdom
{reza,shareeful}@uel.ac.uk,
H.Mouratidis@brighton.ac.uk

Abstract. Safeguarding and securing information assets is critical and challenging for organizations using information system to support their key business processes. *Information Security Management System (ISMS)* defines to setup a solid security framework and regulates systematic way how securely information system can use its resources. However technical advancements of information security do not always guarantee the overall security. All kinds of *human factors* can deeply affect the management of security in an organizational context despite of all security measures. But analyzing, modeling, quantifying and controlling human factors are difficult due to their subjective and context specific nature. This is because individuals tend to have distinct degree of personal and social status. This papers attempts to propose a conceptual framework for analyzing and reasoning three main human factors in an organizational context that supported by goal-modeling language based on concepts of human factors, driving and resisting forces of Force-Field Analysis (FFA) tool, goals, risks, vulnerability, controls, and Threats. This framework is beneficial to better understanding of human factors in the process of ISMS that eventually leads to reasoning a rationale change in organizational context whilst providing reasonable metrics for security. One would be ROI issue that is concern of all organization.

Keywords: Information Security Management System (ISMS), Human Factors, Goal-modeling, Force-Field Analysis (FFA).

1 Introduction

Information Security Management System (ISMS) is necessary prerequisite for business continuity in organizations. To fulfill ISMS goals and objectives, a solid security framework requires ensuring confidentiality, integrity, availability, authenticity and auditability of the critical information assets. Technical mechanism such as authentication mechanism and cryptography, are essential parts of ISMS but people are responsible for design, implementation and operation of these

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 297–305, 2014.

technological tools [1]. At the same time information security systems are highly rule-bound, centrally controlled and it is very exclusive. Bringing all other factors together, create an inclusive environment in which they can be more effective.

Therefore, ISMSs should consider non-technical elements, besides technical elements, in order to be inclusive, cooperative, and communicative whilst invite exploration and promote security satisfaction. Consideration of Human factors enables this but human factors at the same time are the most vulnerable part of the system. Human forces, such as irrational behavior and personal gain can adversely affect the function of security systems. For example, as a result of majority of security password policies that require a complex password from employees, people writing their passwords on the sticky note and attach it to their monitors. This keeps the gate open for intruders to organizations' system. It is important that human factors are addressed at the early stage of system design and in line with ISMS requirements. Information security studies generally focus on the effects of information security with less consideration of security threats quantification, human issues, and clear specification of requirements, which could assist senior management to make decisions on resource allocations and deal effectively with security threats [2][7]. Therefore, organizations remain without clear rationale on specifications of how to achieve information security goals and objectives in regards to human factors, which should have been considered from the early stage of design process. In our previous works [2] we defined direct and indirect human factors and initial analysis of three most influential factors. In this paper first we provide an overview analysis of three influential human factors, Communication, Security Awareness, Management Support and their attributes. Then we provide a meta-model to demonstrate the relationship between human factors and their influences on the control measures, which directly address risks and vulnerabilities. In addition, establishment of the relationship between main human factors and control measures enable ISMS for role-based training and awareness program by defining major human factors.

2 Human Factors of ISMS

The human factor domain is a combination of various disciplines including psychology and ergonomics and tends to optimize human performance in organizations [1]. It is a unique scientific discipline in which people's skills, behavior and restraints are applied together to enhance performance and satisfaction as well as overall achievement of organizational objectives. The dependencies between human factors and their attributes and ISMS goal is shown in figure 1. Figure 1 uniquely links the driving and resisting forces with the goal in terms of its satisfaction and obstruction. The satisfaction of factors and attributes provides goal with support and lack of achievement obstruct goal.

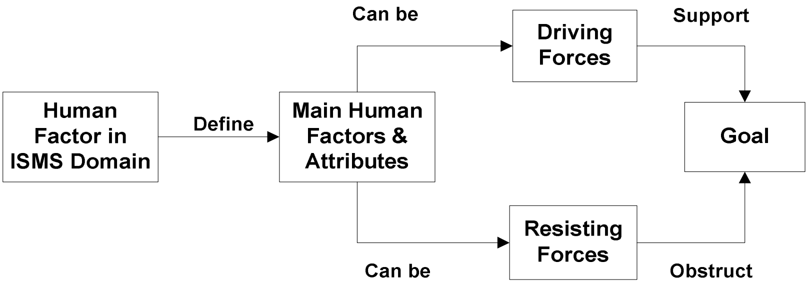

Fig. 1. Dependencies of Human Factor and Goal

There are several researches that highlighted human aspects as main causes of security [2][3][4]. In our previous study, we identified a list of human factors and prioritized three main factors, i.e., security awareness, communication and management support [2]. However the work does not consider the detailed attributes of the identified factors as attributes of human factors. This work provides detailed of these factors, identifying their attributes. Figure 2 provides an overview of three main human factors of ISMS and their attributes. Each single factor also related to other factors as functioning of every factor depends on the effectiveness and integrity of others. We used survey study and Delphi technique for the elicitation and prioritization of the main human factors. Both studies run in two financial organizations.

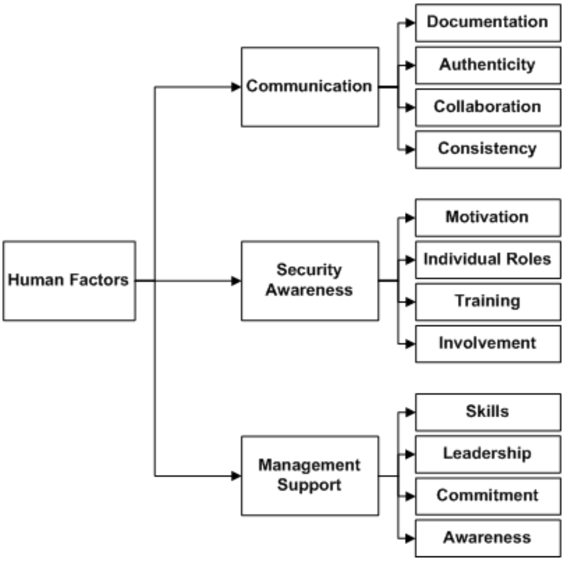

Fig. 2. Human Factors of ISMS

In the proposed conceptual framework we consider a detailed human factors domain analysis and goal-oriented in RE for reasoning the relationship between main human factors and the effectiveness of ISMS. Initially we provide an overview analysis of main human factors and their attributes, and then we present the concepts of the framework.

2.1 Security Awareness

Security Awareness (SA) generally defined as a combination of advising people about information security policies and systems. Awareness also relates to constantly informed around current threats whilst reinforcing acceptable level of IS practices. Organizations have conventionally focused on technical and procedural security measures when implement their information security solutions and proposals [4]. Managing information security risks is greatly depends on forming an effective and convincing awareness culture. Awareness programs' central point is to generate general observation on IS [5]. However, from the information security perspective, this is inadequate because effective IS requires that users being aware of and use the available security measures as outlined in their respective organizations' ISMS policies and mandates. SA consists of the following attributes: ***Motivation:*** achieves stakeholders' willingness to participate in any proposed security policy. ***Involvement:*** ensures all stakeholders are included in the process. ***Individual Roles:*** provides a clear roles and responsibilities of various stakeholders. And finally ***Training:*** deliver all necessary and basic skills and knowledge to the stakeholders. For security awareness becomes a driving force, all attributes must be satisfied.

2.2 Communication

Communication (C) in organizational context is the exchange of messages and ideas between people inside and outside of the organization. The development of information and communication technology has played an important role in computer security [6]. Utilizing users in the direction of compliance with security policy, that is part of ISMS tolls and procedures, can be achieved through effective and persuasive communication. The subsequent effective communication involves reaching all employees in an organization at all levels of its hierarchy. Communication factor composed of the following attributes: ***Authenticity:*** maintains a reliable and necessary communications between stakeholders and ensures all information handled in confidence. ***Documentation:*** produces an audit trail in the communication process amongst stakeholders for the purpose of continuity and consistency. ***Collaboration:*** achieves a coherent and trustworthy communication between stakeholders to support mutual understanding. ***Consistency:*** attains organizations' objectives through stakeholders' steady communication. Achievement of the attributes enables this factor to support goal otherwise the factor would be a resisting factor to obstruct the goal.

2.3 Management Support

Management Support (MS) is essential for effective ISMS [7]. Information security regulations and standards explicitly identified that management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities. The role of management in ISMS is not only to advocate, but also to deliver a clear message of IS security policy to the rest of the organization. The obvious example of management endorsement of ISMS in organizations is the allocation of an adequate budget, which is entirely under the control of senior management. This factor includes the following attributes: ***Awareness:*** This is different from SA that directly deals with the individuals SA. Awareness here defines that senior management must understand and be aware of the importance and necessity of ISMS for their respective organizations. Therefore the awareness of management achieves the objectives of all stakeholders. ***Commitment:*** enables ISMS to be supported by the top organizational hierarchy which important to all stakeholders. ***Skills:*** Absent of technological skills and knowledge in senior management, deprives ISMS goals from a solid strategic information security planning and understanding. ***Leadership:*** is one of the important quality factors for senior management to take the responsibility and ownership of strategic information security vision.

3 Proposed Framework

The proposed framework attempts to analyze human factors in ISMS. We followed and adopted two different techniques to identify our concepts and their attributes, the Force Field Analysis (FFA) and Goal-Modeling (GM). Goal-modeling applicability and its relevance to the organizational context have been of interest of software engineering community in recent years [8] [9]. GM is an early of RE for identifying problems and exploring system solutions and alternative. FFA is a decision-making technique to identify driving and resisting forces concepts involved in addressing goals. We used these two concepts from FFA in Human factors domain analysis assist to define the relationships between ISMS goal and human factors in organizational context (environment) on what the system is supposed to do and why. Goal in GM and FFA is an integration point of the concepts of these two techniques. Next section provides a definition of concepts based on this proposed framework.

3.1 Conceptual Model

Conceptual models are formed by concepts for understanding theme they depict [11]. Therefore, the concepts require be defining and presenting by examples. We use different concepts that are relevant for analyzing human factors. We follow force-field analysis and goal-modeling language for this purpose. The following concepts are important for analyzing human factors in ISMS:

- ***Human factor***: Human factor is a unique discipline for optimization of human performance in organizations for achievement of organizational objectives. We identified three main human factors in our previous studies, which has four attributes. Each of these factors can be either driving forces or resisting factors.

Awareness, Management Support and Communication are the examples of human factor and each of them are followed by four attributes as mentioned previously. Factors can be driving or resisting forces depending the value of the attributes. If the attributes are adequate or true then the relevant factor is driving forces otherwise they are resisting forces that obstruct goals.

- ***Driving forces*****:** Driving forces are the forces in organizational context that support change in the desired. Each identified human factors can be a driving force if all attributes are true and achieved. For example, if management support achieves all necessary attributes including skills, leadership, commitment and awareness then it becomes a driving force that supports the goal. Lack of management support can affect the allocation of budget that is essential for the continuity of security enforcement.
- ***Resisting forces:*** They are forces that oppose the positive changes and intending to keep the statue quo or current situation. Human factors become a resisting force if all attributes are false and failed to achieve. For example, E-mail as a communication tool could potentially become a resisting force. Authenticity is one of the attributes of communication and if it is not achieved then obstructs the goal.
- ***Goal:*** is a high-level objective for achievement that provides a framework for desired system in organizations. In ISMS goal contribute to the achievement of a process to ensure the confidentiality, integrity, availability, authenticity and audibility of the critical information assets in organizational context. For example, to eliminate possible loss and disruption of information due to compromised network for achieving a high level desire of reputational damage.
- ***Vulnerability:*** is a weakness in system that allows the integrity of system to be violated. For example, SA becomes a resisting force and creates vulnerability if lack of adequate training leads to use of weak password combination by users and pose a potential risk of unauthorized access.
- ***Threat:*** A Threat is potentially harmful activities that cause destruction, disclosure, modification and/or loss of data [10]. However, specific weakness doesn't create threat but the existing of information systems facilitates threats. Vulnerabilities are contributing to the threats. Threats are pervasive and complex in nature and can be classified as follows: ***Internal*** and ***External*** agents. The internal threats cause risks to organizations mainly through employees. Examples are, use of mobile devices or misused of privilege access to system. Examples of external threats can be the theft of employees' mobile devices.
- ***Risk:*** ISO standard defined risk as a combination of the probability of an event and its consequence [12]. In our meta-model vulnerabilities and threats contribute to risks. Risk is the outcome of the threat multiplies by probability and business impact. An example of risk would be when personal information is passed to unauthorized person.
- ***Control:*** is defined as any technical and non-technical measure or method that is used for addressing vulnerabilities and influencing human factors in our framework. For example, the support of management is an important factor in the process of ISMS that has been noted in ISO standards but to ensure this is an achievable control the attributes of this control that we listed above should be fulfilled. Control also contribute to the return of investment (ROI) as security expenditure are become an important matter for organizations.

Figure 3 demonstrates the meta-model that combine and model all the defined core concepts in this paper. The objective of this meta-model is to demonstrate and represent: a) main human factors attributes and, b) to demonstrate the relationship between these attributes and control measures in regards to risks and vulnerabilities. The meta-model is used as a technique to structure to analyze human factors in ISMS in a conditioned way so that it can be addressed to meet organizational needs. In this model, human factor is the main concept that consists of three main factors. Each factor has four attributes. If attributes of a factor are fulfilled then the factor becomes a driving force concept that supports goal otherwise it becomes a resisting force, which obstruct the goal concept. For example, the Management Support factor can only be a driving force and support the goal if the management commitment is achieved as well as other attributes. Giving a scenario in which an organization has a solid security policy in place and achieved a security credential, however, senior management is not committed to allocate adequate budget to fulfill the security goals. Lack of budget obstructing goal and creates vulnerability such as, exploiting users weaknesses using social engineering methods. Vulnerability contributes to a potential risk whilst threat causes risk. This risk could be loss of confidential data or reputation damage. In order organizations address vulnerabilities and potential risks, controls are recommended to address the vulnerabilities and risks and meet organizational requirements. This shows the dependency of controls to human factors and therefore controls influence human factors. An example of control would be recognition of adequate training program that conform to each individual organization considering that selection of appropriate and cost effective control itself can be a complex and subjective process. The evidence of the meta-model is the effect of the human factors'

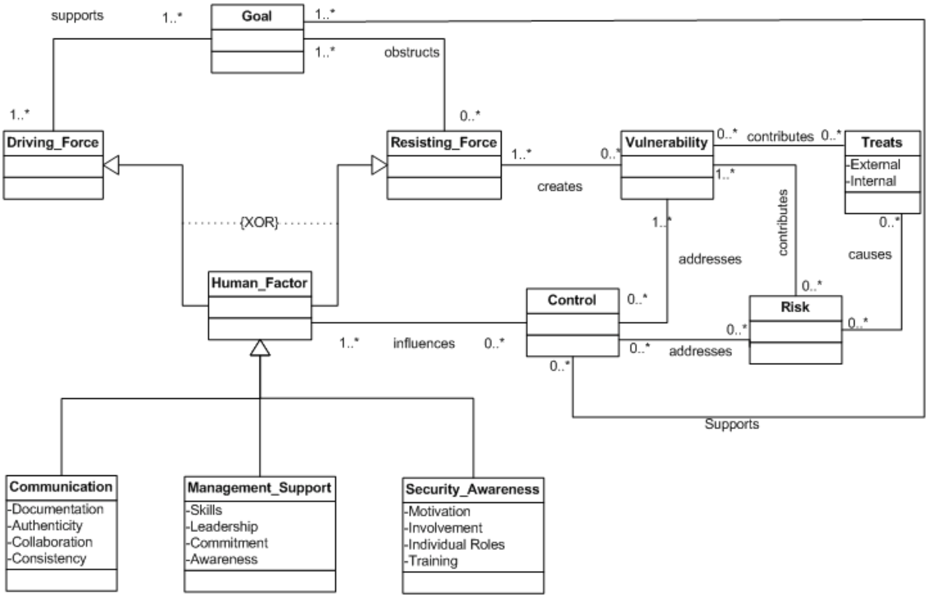

Fig. 3. Meta-model

attributes on individual roles in organizations. Decisions made about controls influence by role-based individuals in various positions, which derived from human factors' attributes. Any control measures assigned to address risks must be affiliated and appropriate to individuals concerning attributes of main factors. The main benefit of this metal model is to analyze and reveals major issues of conflicting desires and expectations in ISMS, which leads to reasoning a rationale change in organizational context. One would be ROI issue that is concern of all organization.

4 Conclusion

Our paper underlines the importance of understanding of main human factors in the effectiveness of ISMS. The proposed conceptual goal-modeling framework attempts to provide ISMS requirements and other related concepts. This framework provides a unique understanding of forces that promotes security posture and satisfaction of ISMS goals in organizational context. Conceptual framework of human domain analysis and GM contribute to the mitigation of risks and the effectiveness of ISMS in organizations. Our future work will be evaluating the proposed framework in two case studies to ensure that the framework can be generalized across the organizational context in real world cases as well as expansion of this work to two major areas of Information Security Assurance (ISA) and Return of Investment (ROI) and their concepts.

References

1. Lacey, D.: Managing the Human Factor in Information Security, How to win over staff and influence business managers. John Wiley & Sons Ltd., Chichester (2009)
2. Alavi, R., Islam, S., Jahankhani, H., Al-Nemrat, A.: Analyzing Human Factors for an Effective Information Security Management System. International Journal Of Secure Software Engineering (IJSSE) 4, 50–75 (2013)
3. Lee, J., Lee, Y.: A holistic model of computer abuse within organizations. Information Management & Computer Security 10(2/3), 57–63 (2002)
4. Puhakainen, P.: Design Theory for Information Security Awareness. University of Oulu, Oulu (2006)
5. Wilson, M., Hash, J.: Building an Information Technology Security Awareness and Training Program. U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Washington (2003)
6. Dhillon, G., Backhouse, J.: Information system security management in the new millennium. Communications of the ACM 43(7), 125–128 (2000)
7. Reddick, C.G.: Management support and information security: an empirical study of Texas state agencies in the USA. Electronic Government, An International Journal 6, 361–377 (2009)
8. Islam, S., Houmb, S.H.: Integrating Risk Management Activities into Requirements Engineering. In: Proceeding of the 4th IEEE International Conference on Research Challenges in Information Science (RCIS 2010), Nice, France (2010)

9. Islam, S., Mouratidis, H., Weippl, E.: An Empirical Study on the Implementation and Evaluation of a Goal-driven Software Development Risk Management Model. Journal of Information and Software Technology 56(2) (February 2014)
10. Mattord, J., Whitman, M.: Management of Information Security, 2nd edn. Thomson Learning Inc., Canada (2008)
11. Mouratidis, H., Giorgini, P.: Integrating Security and Software Engineering: Advances and Future Visions. Idea Group Publication (2007)
12. ISO/IEC: Information technology - Security techniques - Information security management systems - Overview and Vocabulary. ISO/IEC 27000, International Organization for Standardization (ISO) and International Electro technical Commission (IEC) (2009)