2012

A MODEL FOR EVALUATING INFORMATION SECURITY WITH A FOCUS ON THE USER

Lucio Silva
Ufpe, lucio_camara@hotmail.com

Silvio Menezes
Ufpe, silvio_recife@yahoo.com.br

Ana Paula Cabral Seixas Costa
Ufpe, apcabral@hotmail.com

A MODEL FOR EVALUATING INFORMATION SECURITY WITH A FOCUS ON THE USER

Silva, Lúcio, Federal University of Pernambuco, Recife PE, 5125, Brazil, lucio_camara@hotmail.com

Menezes, Silvio, Federal University of Pernambuco, Recife PE, 5125, Brazil, silvio_recife@yahoo.com.br

Costa, Ana Paula Cabral, Federal University of Pernambuco, Recife PE, 5125, Brazil, apcabral@hotmail.com

Abstract

This study presents a theoretical model to evaluate the level of information security in an organisational environment with a focus on the knowledge, attitudes and behaviour of the end-user, identifying the level and origin of the gap between the information security guidelines laid down by the company and the actual practices of its internal staff, third party partners and suppliers. The model is designed to assist in meeting the objectives and policies set for the management of information security by senior management and contributes to maintaining an effective training programme as well as to raising awareness on information security.

Keywords: Information Security, Security Policies, User.

1 INTRODUCTION

During the last twenty years or so, several methodologies have been developed to evaluate information security and the maturity of security (Albrechtsena and Hovdena 2009; Ashenden 2008; Hyun et al. 2009; Rhee et al. 2009). Many issues have been addressed, such as the processes of product design, the setting of business strategies and information security management; thus, the role of the end-user in the field of information security has been emphasised.

As organisations are becoming more dependent on information technology, researchers encourage managers to give more serious consideration to the role of human resources in the field of managing information security (Wipawayangkool, 2010). According to Yayla (2011), user errors and negligence are arguably the two most common unintentional insider threats. Some of the underlying reasons behind user errors are lack of experience in utilising security tools, complexity of the security tools and job stress due to time pressure and workload (Yayla, 2011).

Therefore, the success of information security management depends on appropriate information security aspects, such as the factors influencing the end-user security behaviour, challenges in achieving compliance and good communication among Information Security Managers, end-users and Senior Managers (Ashenden,2008; Rhee et al,2009). In this way, according to Puhakainen & Siponen (2010), a key factor in information system problem in organisations is the user noncompliance with IS security policies. Therefore, activities such as training, pay practices and motivating people to strengthen security efforts can support information security programmes more effectively (Rhee et al. 2009; Wipawayangkool. 2010).

Regarding IS security training, the literature (Peltier, 2002) suggests incorporating a pedagogical orientation as a key factor in improving user compliance with IS security policies. Given the importance of the human perspective as reported in the literature in recent years and once pedagogy is related to behaviour, this paper puts forward a model to evaluate the level of Information Security with a focus on the knowledge and behaviour of the end-user. The model is designed to assist in meeting the objectives and policies set for the management of information security by senior management and contributes to maintaining an effective training programme as well as to raising awareness on information security.

The present study is organised as follows: in section two, the authors describe factors affecting security behaviour of users identified in the literature; in section three, a model to help staff achieve a high level of compliance with the information security policy (ISP) of the organisation is proposed; section four illustrates the applicability of our methodology by using a hypothetical case study. The article concludes by discussing advantages and limitations of the model.

2 HUMAN AND ORGANISATIONAL FACTORS IN INFORMATION SECURITY

Because organisational environments present users with numerous choices in using personal computers that might support or deter information security best practices (Abraham, 2011), studies on human and organisational aspects are greatly outnumbered by studies on technological advances (Beznosov and Beznosova, 2007). Thus, human aspects have been receiving particular attention in research studies and business practices because of the fundamental role of the users.

Abraham (2011) presents an extensive literature review on information security behaviour in the context of factors affecting security behaviour of users in organisational environments. These factors were organised by utilising the conceptual model proposed by Leach (2003), as described in Table 1 below.

Category	Description	Themes
The body of knowledge	What employees are told and come to know about security best practices in an organisation	Security Policies, Communication Practices and Content of Awareness Efforts
What they see in practice in the organisation	What employees see in practice around them in the organisation	Management Influences, Peer Influences, Deterrence Efforts, Rewards and Employee Participation.
User's security common sense and decision making skills	Factors affecting security behaviour of users in terms of the user's security knowledge	User's Knowledge and Self-Efficacy
The user's personal values and standard of conduct	Factors affecting security behaviour of users based on the user's personal values, beliefs and standard of conduct	Attitudes and Beliefs
The user's psychological contract with employer	Unwritten reciprocal agreement existing between employee and employer to act in each other's interests	Psychological Ownership, Organisational Commitment, Trust and Procedural Justice
Effort required for compliance and temptation not to comply	The influence of the degree to which organisations make it easy for their employees to adhere to security standards and procedures	Ease of Use and Effectiveness of Security Technology

Table 1. Factors Affecting Security Behaviour of Users

In order to emphasise the factors identified, this paper presents some other studies. According to Albrechtsena and Hovdena (2009), there is a limited interaction between users and information security managers, resulting in divergent views and interpretations of information security. This explains why managers and users claim that there is a digital division between such groups in terms of their views and experience in information security practices.

In this way, Eminagaoglu et al (2009) consider an appropriate integration of people, process and technology as important factors for information security management to be successful. In their paper, the authors demonstrate that when proper integration comes to the issue of people, this effectiveness can be achieved through security awareness training of employees. However, the authors point out that the outcomes should also be measured in order to assess how successful and effective this training has been for the employees. Dlaminia et al (2009) reinforce this problem, considering the need to minimise the gap between regulatory issues and practices in the technical implementation of information security.

Tudor (2001) presents a security training programme which includes phases such as: developing and scheduling training targeted at executive level management; assessing security policies, procedures and guidelines; identifying strategic information, sources and mission critical systems; establishing a security awareness and training programme committee; reviewing and recommending security tools; establishing emergency as well as incident response and reporting procedures; schedule training; identifying communication methods; determining security awareness promotional activities; and integrating security into organisational processes.

Knowing the importance of the employee, Veiga and Eloff (2010) affirm that information security policies should focus on employee behaviour. According to them, an information-security-aware culture will reduce the risk of employee misbehaviour. Martins and Eloff (2001) set out how organisational culture influences the way things are done in an organisation and, therefore, how this is related to the behaviour and attitudes of people. Attitude is what people feel and how they would behave in certain circumstances, while behaviour is determined by what people would like to do, and what they think they should do. In other words, attitude is understood as the intent and coherence in what and how to think, feel and react in relation to something or someone. Behaviour is the action,

consisting of the change, movement or reaction of any entity or system in relation to its environment or situation.

Yayla (2011) proposes a framework for controlling insider threats, which can be categorised as intentional and unintentional, to information security. In order to mitigate intentional insider threats, the proposed framework draws connections to the organisational behaviour, criminology and psychology literature by increasing employees' integration and commitment, using deterrent measures and implementing technology-based controls. On the other hand, unintentional threats can be controlled or mitigated by increasing employees' intrinsic motivation, providing training in security tools, implementing security tools with high level of usability, adjusting time pressure and workload on employees, and finally by increasing awareness among users and management.

Considering the importance and need for organisations to measure and report on the state of the information security culture within their business, as seen earlier, this paper puts forward a set of policies that enables the level of maturity of information security to be gauged in the organisation, based on the knowledge and behaviour (K - knowledge, B - behaviour) of individuals with regard to the (ISP) of the organisation.

3 THE PROPOSED EVALUATION MODEL

In order to analyse the level of compliance with the ISP of the organisation, the present work proposes a model that identifies assesses and defines the status of compliance with corporate security policy.

The model assumes that the company uses the resources of Information Technology (IT) and has laid down an ISP and a Training and Awareness Programme. The model proposed suggests the development of three phases: Structuring, Modelling and Evaluation, as can be seen in Figure 1.

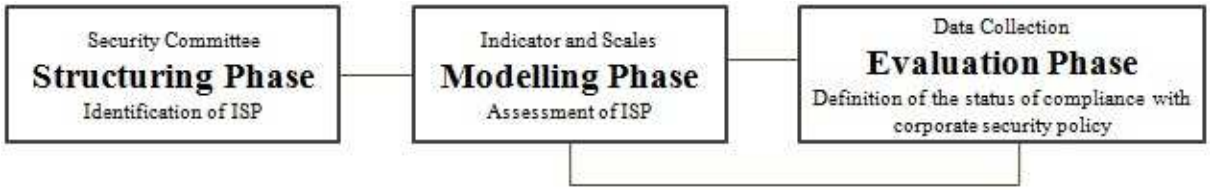

Figure 1. Phases of the Model

3.1 Model Description

In the Structuring Phase, what must be created, if not already there, is a Security Committee: a group that includes representatives from all areas of the company, who will discuss topics focused on security, dealing with technical skills and guided by policy. In this moment, the ISP must be identified. This Policy will guide the next phases of the model, which may also be adjusted depending on the outcomes of those phases.

The next phase, the Modelling Phase, focuses on the choice of indicators and scales of analysis that will assess the extent of staff compliance within a company´s information security policy. The achievement of goals depends on choosing indicators that effectively reflect the fulfilment of the organisation's security guidelines.

The last phase is used to collect data, calculate the indicators and analyse the results individually and as a whole so as to determine if the corrective actions in pursuit of improved performance have been effective. In general, this phase defines the status of compliance with the corporate security policy.

It should be noted that the Structuring and Modelling phases would be performed primarily once and revisited only periodically as policies are modified, while the Evaluation phase would be performed periodically to continually assess how well the organisation is in compliance with its security policies.

3.2 Identification of indicators

The evaluation of information security with a focus on the user seeks to reduce user noncompliance with IS security policies. In this way, this paper puts forward a set of indicators, based on the literature, which can be used in evaluating compliance with a company´s information security policy.

Some findings obtained from Puhakainen & Siponen (2010) and the phases presented in Tudor (2001) were useful to build our set of indicators. The indicators used should be in accordance with the company's business objectives. Table 3 shows such indicators and the relationship of each with K - knowledge, B - behaviour of the end-user in terms of the company´s Security Policy. Knowledge (K) is associated with understanding of each end-user; consequently, the training and awareness programme has an important influence on those indicators. Behaviour (B) is associated with the concern and intention to preserve and protect the organisation's information technology and resources.

3.3 Performance measures

The task of establishing performance objectives in order to identify whether these are efficiency indicators is complex because there are aspects that do not attract measurable numerical values, although these aspects can clearly show if there has been an improvement in performance. In many such cases, if necessary, numerical values can be assigned subjectively. Thus, a company may establish rating scales for the indicators individually and globally, but it should be ready to adjust them in the course of their use.

In William and Gholamreza (1988), the researchers conducted a factor analysis and the results suggest a 12-item instrument that measures five components to end-user satisfaction that could be adapted to measure the performance of end-user training.

Based on what was reported in the literature, it is suggested that special attention be given to evaluating training and awareness-raising programmes already carried out. According to RadhaKanta and Vincent (2005), training programmes help create a computer-literate workforce. The researchers have addressed this issue by designing, testing, and presenting a comprehensive framework for evaluating end-user training programmes. The manager can design their own end-user training-evaluation process as a feedback system for monitoring training effectiveness and generate the information needed to improve the training programmes.

In this study, the training-evaluation process is proposed, based on the most common themes in security training programmes. According to a survey conducted by the ENISA (European Network and Information Security Agency), these themes are internet security, responsibility for information security, reporting security incidents, security updates and applying patches, personal use of company equipment, e-mail. Thus, these themes can be used to evaluate the use of individual end-user training programme and awareness-raising events.

The overall average recovery of each end-user in the training programme and awareness-raising sessions should be represented by PI-23, according to Table 2. However, depending on the average training set as satisfactory by the organisation for each individual, PI-23 may indicate that users must schedule re-taking the training with a view to improving their performance.

As mentioned earlier, the indicators were proposed based on literature and their calculation attempts to be simple in order to be developed and useful for the company routine. Table 2 shows, where appropriate, the mathematical expression used to obtain each indicator and the scales suggested, in order to illustrate the application of the proposed model.

	Indicator	Calculation of indicator	Assessment of individual performance indicators	
			K (weight =0.4)	B (weight=0.6)
PI1	Information Security is updated	Yes or No	If it is, it is equal to 100 If it isn´t 0	If it is, it is equal to 100 If it isn´t 0
PI2	Active and public support from top	Yes or No	-	If it is given, it is equal to 100

	management			If it isn´t 0
PI3	End-users know of the existence of the Security Policy	% = (No. of positive answers from staff already surveyed / Total no. of staff in the company) x 100	%	-
PI4	Reading Policy	% = (No. of staff who answered questions related to Security Policy / Total no. of staff in the company) x 100	%	-
PI5	End-users demonstrate knowledge of the Policy	% = (No. of staff who had a satisfactory score in tests which demonstrate their knowledge of the policy / Total no. of staff in the company) x 100	%	-
PI6	Understanding to whom to report incidents.	%= (No. of staff who answered this question correctly in tests / Total no. of staff in the company) x 100	%	-
PI7	Threat / Warning	Δtmin= t2 – t1 Where: t2 is the instant of receiving the warning; t1 is the instant of discovering the threat.	If 0<Δt=<15min, so n= 100; If 15<Δt<=60 min, so n= 50; If Δt>60min, so n=0	If 0<Δt=<15min so n= 100; If 15<Δt<=60 min, so n= 50; If Δt>60min, so n=0
PI8	End-users participating in security training	% = (No of staff who take part in training / Total no. of staff in the company) x 100	-	%
PI9	Elapsed time between training of the end-user related to security	Δtdays= t2 – t1 Where: t2 is the date of the last training event; t1 is the date of the previous training event.	If 0<Δt<90 days, so n= 100; If 91< Δt<=180 days, so n= 50; If Δt>180 days, so n=0	-
PI10	Non-compliance with security policy	Δ% = ((N.C.2 /N.C.1)-1) x 100 Where: N.C.2 is the number of Non-Conformities in the last audit. N.C.1 is the number of Non-Conformities in the previous audit.	If Δ<0%, so n= 100; If Δ>=0% and Δ<10%, so n= 50; If Δ>10%, so n=0	If Δ<0% so n= 100; If Δ>=0% and Δ<10%, so n= 50; If Δ>10%, so n=0
PI11	Involvement of end-user	% = (No. of staff who demonstrate their involvement with the scenario of the tests / Total no. of staff who took the tests) x 100	%	-
PI12	Recognition of events in testing	% = (No. of staff who obtained a satisfactory score which may demonstrate recognition of events in tests / Total no. of staff who took the tests) x 100	%	-
PI13	Test failed to reveal password	% = (No of staff who failed to reveal their password in tests / Total no. of staff who took the tests) x 100	(100-%)	(100-%)
PI14	Results of searches for viruses and unauthorised software.	Δ% = ((P2 /P1)-1) x 100 Where: P2 is the total number of searches for viruses added to the number of unauthorised software programmes set up on internal workstations and mobile equipment, obtained from the last survey.	If Δ%<0, so n= 100; If Δ%>=0 and Δ%<10, so n= 50; If Δ%>10, so n=0	If Δ%<0, so n= 100; If Δ%>=0 and Δ%<10, so n= 50; If Δ%>10, so n=0

		P1 is the total number of searches for viruses added to the number of unauthorised software programmes set up on internal workstations and mobile equipment, obtained from the last but one survey.		
PI15.1	The source of security incidents experienced lies in human behaviour	% = (No of incidents arising from inappropriate behaviour by an employee / Total no. of incidents in the period) x 100	(100 - %)	(100 - %)
PI15.2	Downtime due to incidents arising from human behaviour	% = (Downtime due to incident arising from human behaviour in the company as a whole in a given period / Total downtime in the period) x 100	(100 - %)	(100 - %)
PI16	Partners and suppliers re-evaluated in terms of their awareness of and practices in security	% = (No. of suppliers and partners re-assessed as to aspects of security and awareness-raising / Total no. of partners and suppliers) x 100	%	%
PI17	Critical data strongly protected	% = (No. of pieces of data identified as critical which are strongly protected / Total no. of critical data items in the company) x 100	-	%
PI18	Spyware installed in stations	% = (Total amount of spyware detected in workstations / Total no. of workstations and mobile devices subject to spyware in the organisation) x 100	(100 – %)	(100 – %)
PI19	Waste paper shredded	Percentage of paper shredded in the survey: %Pf = ΣQu / Qf Where: ΣQu = (No. of sheets used by the Dept /User x (Area of the sheet in mm2) /100,000) x Weight of 1 sheet in Kg per m2 or ΣQu = (No. of copies from the Dept/ User x (Area of the sheet in mm2) /100.000) x Weight of 1 sheet in Kg per m2 Qf = Weight in Kg of all the shredded paper collected in the period separately.	%	%
PI20	Illegal traffic on the internal network	% = (Volume in bytes of illegal traffic, accounted for by the PIS / Total traffic in bytes in the organisation) x 100	-	(100 - %)
PI21	Weak user passwords	% = (No. of weak passwords / Total no. of passwords registered in the organisation) x 100	(100 - %)	(100 - %)
PI22	Requests to the security department	Δ% = ((NSol2 /NSol1)-1) x 100 Where: NSol2 is the number of requests to the department from the last survey. NSol1 is the number of requests to the department from the last but one	If Δ%<0, so n= 100; If Δ%>=0 and Δ%<10, so n= 50; If Δ%>10, so	If Δ%<0, so n= 100; If Δ%>=0 and Δ%<10, so n= 50; If Δ%>10, so

		survey.	n=0	n=0
PI23	Global Average of Test Scores	Mathematical average of the results of the tests received by all the staff who took them.	If 0<=Xtests<=4,9, so n=0 If 5<=Xtests <=6,9, so n=50 If 7<=Xtests<=10, so n=100	-
AVERAGE			X_K	X_B

Table 2. Performance Indicator

The values obtained for each indicator must be processed in order to inform the status of compliance with corporate security policy as presented in Table 3. As one should note, this process occurs during the evaluation phase.

Level	Description
GOOD - Keep	Good level of performance or knowledge of the aspect.
REGULAR - Monitor and Improve	There is some level of performance or knowledge regarding the appearance compliance, but it is not yet rated as satisfactory; constant monitoring and improvements to be planned for is required.
BAD – Urgent Operation	There is no compliance or knowledge concerning the evaluated aspect; urgent intervention required.

Table 3. Level of compliance with the Performance Indicators (PI)

Finally, in order to attribute the percentage of each indicator, Table 2 also shows what the evaluation of individual performance indicators for knowledge (K) and behaviour (B) is like, considering its limits and weights.

The 'behaviour' aspect received the most weight (0.6), since this is a fundamental aspect for implementing an Information Security Policy, while 'knowledge', which gives the necessary support to the end-user, received 0.4. The values given to those weights must be specific for each organisation. Thus, the results of the related levels should support each organisation, so that action can be taken and adjustments made to the adopted policies, making them tougher as far as Information Security is concerned.

For a comprehensive assessment of the organisation, a calculation must be made of the weighed average of the performance indicators as per Expression 1.

$$X = ((X_K \times 0.4) + (X_B \times 0.6)) / 100 \quad (1)$$

Table 4 presents an illustration of this global evaluation, which depends on the value of X (Expression 1).

Level	Description
70% <= X <= 100%	Good level of adherence of end-users to the Information Security Policy of the organisation.
50% <= X <= 69%	There is some level of adherence by end-users to the Information Security policy of the organisation, but it is not satisfactory; constant monitoring and planning improvements are required.
0% <= X <= 49%	End-users do not adhere to the Information Security Policy of the organisation; this requires urgent intervention.

Table 4. Global Assessment of the level of compliance with Information Security Policy

Finally, this information serves as a warning to the organisation, so that it may take appropriate action, once employees who do not comply with information security policies are a serious risk for their companies (Puhakainen & Siponen, 2010).

4 CONCLUSION AND FUTURE RESEARCH

In this paper, a model was put forward to help managers, whether directly or indirectly responsible for information security in the organisation, to identify the level and origin of the gap between the information security guidelines laid down by the company and the actual practices of its internal staff, third party partners and suppliers. The model is designed to assist in meeting the objectives and policies set for the management of information security by senior management, and contributes to maintaining an effective training programme and in raising awareness on information security.

This paper does not claim to identify accurately, by means of quantitative analysis, how secure the company is, but to influence individuals to create opportunities for improving Security Policy, Awareness-Raising and Training Programmes, aimed at reducing the risks associated with the use of information resources by individuals. This is made possible by using a mechanism for setting assessment indicators which use individual and global scales.

Many challenges remain for future research in this area. Developing a questionnaire to be applied in some organisations is quite a good solution to validate our model. Using a large number of companies may lead to include other aspects related to this subject, reinforcing the model.

References

Abraham, S. (2011). Information Security Behaviours: Factors and Researches Directions, Proceedings of the 17th Americas Conference on Information Systems (AMCIS), Detroit, Michigan.

Albrechtsena , E. Hovdena, J. (2009). The information security digital divide between information security managers and users. Computers & Security, Vol. 28 No. 6, 476–490.

Ashenden , D.(2008). Information Security management: A human challenge?. Information Security Technical Report, 13, 195–201.

Beznosov, K. and Beznosova, O. (2007), On the imbalance of the security problem space and its expected consequences. Information Management & Computer Security, Vol. 15 No. 5, pp. 420-31.

Dlaminia, M.T. Eloffa, J.H.P. Eloffb, M.M. (2009). Information security: The moving target. Computers & Security, 28, 189–198.

Eminagaoglu, M. Ucar, E. Eren, S. (2009). The positive outcomes of information security awareness training in companies: A case study. Information Security Technical Report, 14, 223-229.

ENISA – European Network and Information Security Agency. Available at: http://www.enisa.europa.eu/

Hyun, M. Kim, T-S. Kong, H-K. Yoo, H-W. (2010). A Balanced Scorecard Approach to Evaluate Corporate Information Security Level and Suggestion of a Security Maturity Model. Proceedings of the 16th Americas Conference on Information Systems (AMCIS) Lima, Peru.

Leach, J. (2003). Improving User Security Behavior. Computers & Security, 22 (8).

Martins, A. and Eloff, J. (2001). Measuring Information Security. Online: http://www.acsac.org/measurement/positionpapers/martins.pdf.

Peltier, T. (2002). How to Build a Comprehensive Security Awareness Programme. Computer Security Journal (16:2), pp. 23-32.

Puhakainen, P. and Siponen, M. (2010) Improving employees' compliance through information systems security training: an action research study. MIS Quarterly, 34 (4), 757-778.

RadhaKanta M. and Vincent S. L. (2005). Evaluating end-user training programmes. Commun. ACM, 48 (1), 66-70.

Rheea, H.S. Kim, C. Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end-users' information security practice behaviour. Computers & Security, 28, 816–826.

Tudor, J. K. (2001). IS Security Architecture: An Integrated Approach to Security in the Organisation, Boca Raton, FL: Auerbach Publications.

Veiga, A. Da, Eloff, J.H.P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29, 196–207

Yayla, A. (2011). Controlling insider threats with information security policies. Proceedings of the 19th European Conference on Information Systems (ECIS), Helsinki-Finland.
William J. D. and Gholamreza T. (1988). The measurement of end-user computing satisfaction. MIS Quarterly Vol. 12, No. 2 (Jun., 1988), pp. 259-274
Wipawayangkool, K. (2010). Strategic Role of Human Resource Management in Information Security Management. Proceedings of the 16th Americas Conference on Information Systems (AMCIS), Lima-Peru.