Web Banking: A Security Management and Communications Approach

Ioannis Koskosas

School of Economics and Business Administration
International Hellenic University-IHU
14th km Thessaloniki-Moudania, 57001, Thermi, Greece
Tel: +3 2310 807528
e-mail : ioanniskoskosas@yahoo.com

Abstract

The paper provides a survey research report on the information security and communication management disciplines within the scope of Web Banking. The benefits and uses of information and communication approaches were examined to determine their influence on the effective management of web banking security risks. Information and communication approaches have not changed the structure of security management, but have enabled new forms of employees' collaboration and provided higher and more efficient project task productivity as defined by the survey. Achieving the required level of security management requires an effective communication policy, security awareness and control and measures tailored to the new organizational needs based on rapid web banking technology.

Keywords: Web banking, security management, communication policy, information systems.

1. Introduction

Although the various aspects of information security may have been studied for many years, the social aspects of information security in the banking sector through electronic channels such as the web, have appeared in the information systems (IS) literature since the late 1990s (Devlin, 1995; Buhl and Will, 1998; Hoffman et al., 1999, Palmer et al., 2000). E-commerce is still moving rapidly, and its further ahead of the human time; time necessary to build such reflective security management procedures and tools that will allow users to trust e-commerce based services and products such as web banking. Communication should be a key to e-commerce (Keen et al., 2000) because it is crucial in cases of risk, uncertainty and interdependence. This association has not yet been translated in the electronic world to its full potential. Banks are reluctant to adopt security communication tools that will improve more effectively the management of web banking products and services offered to their customers.

The reliance by every organization upon information technology (IT) has increased dramatically, as technology has developed and evolved simultaneously to e-commerce. Over recent decades, organizations have come to depend on IT for operations, external transactions, and mediated communications (e.g., e-mail, fascimile). Similarly, information has developed into a strategic asset, while the computerized information systems have become ultimate strategic tools for both government and organizations (McCumber, 2005; Sherwood et.al, 2005). Due to globalization and competitive economic environments, efficient information management is critical to business survival and effective decision making activities. Although, as connectivity to devices has increased, so has the likelihood of unauthorized intrusion to systems, theft, defacement, and other forms of information resource loss. However, information systems are deeply exposed to security threats as organizations push their technological resources to the limit in order to meet organizational needs (Dhillon, 2001; Dhillon and Torkzadeh, 2006).

To this end, the aim of this research is to examine the existence and use of information and communication approaches, for the management of web banking security-related risks, based on a survey report of a single case study. The main research assumption is that the existence of effective information and communication approaches would relate positively to the enactment of web banking security-related approaches that will further establish the trust of customers in using web banking products and services. Hence, effective information and communication approaches must support the mission of the banks with regard to web banking security; they must provide more effective security procedures, measures and controls in safeguarding web banking and be in sync with the bank's ultimate business scope which is enhancing trust to customers in using web banking.

2. Theoretical framework

2.1 Web banking trends

Web banking is gaining ground every single day although security threats using its products and services remain high and discourage people from using them more frequently or using them at all! Banks have started to operate their new websites through which their customers not only inquire account balances but also have the ability to check interest and exchange rates and also to conduct a wide range of other transactions such as money transfer, bill payments, etc. Unfortunately, data in e-banking are scarce and differences in definitions make cross countries difficult. However, web banking is particularly widespread in Scandinavian countries, Spain and Switzerland where more than 75 percent of all banks offer such services (Claessens et al., 2002).

To date, most of the banks combine the new electronic delivery channels with traditional brick and mortar branches but a small number has emerged that offer their products and services predominantly through electronic distribution channels. These banks may have not a branch network but might have a physical presence, an administrative office or ATMs. Also most industries have been influenced, in one way or another, by this promising new technology (Gunasekaran and Love, 1999). However, customers have not adopted B2C e-commerce and e-banking in the same degree (Hoffman et al., 1999) mainly due to security threats (Palmer et al., 2000) and trust related issues (Lee and Turban, 2001). Customers simply have not enough trust on most online services in order engage with them.

The focus of e-banking services is in selling and serving customers at a rapid pace. In effect, these businesses have invested in interactive information systems with the expectation that it will contribute to their overall profit and market share. Similarly, customers are dealing with online products and services that are becoming increasingly sophisticated from a technological point of view. However, there will be a minimum return from such investments if banks fail to communicate and share information among customers so that fully to utilise their activities.

2.2 Information security trends

Although a number of IS security approaches have been developed over the years that reactively minimize security threats such as checklists, risk analysis and evaluation methods, there is a need to establish mechanisms to proactively manage IS security. That said, academics' and practitioners' interest has turned on social and organizational factors that may have an influence on IS security development and management. For example, Orlikowski and Gash (1994) have emphasized the importance of understanding the assumptions and values of different stakeholders to successful IS implementation. Such values have also been considered important in organizational change (Simpson and Wilson, 1999), in security planning (Straub and Welke, 1998) and in identifying the values of internet commerce to customers (Keeney, 1999).

Dhillon and Torkzadeh (2006) have also used the value-focused thinking approach to identify fundamental and mean objectives, as opposed to goals, that would be a basis for developing IS security measures. These value-focused objectives were more of the organizational and contextual type.

A number of studies investigated inter-organizational trust in a technical context. Some of them have studied the impacts of trust in an e-commerce context (Gefen et al., 2003; Gefen and Straub, 2004; McKnight et al., 2002) and others in virtual teams (Ridings et al., 2002; Sarker et al., 2003). Workman (2007) studied trust as a factor in social engineering threat success and found that people who were trusting were more likely to fall victims to social engineering than those who were distrusting. Koskosas (2009) used a risk communication approach to identify weaknesses in information systems security development procedures in terms of a possible communication breakdown among organizational employees in communicating security goals efficiently.

However, information security from a social point of view is part of the corporate culture and defines how employees see the organization (Sherwood et al., 2003). Organizational culture is a system of learned behavior which is reflected on the level of end-user awareness and can have an effect on the success or failure of the information security process. Albrechtsen (2006) found that users considered a user-involving approach to be much more effective for influencing user awareness and behavior in information security. Leach (2003) studied influences that affect a user's security behavior and suggested that by strengthening security culture organizations may have significant security gains. Debar and Viinikka (2006) investigated security information management as an outsourced service and suggested augmenting security procedures as a solution, while von Solms and von Solms (2004) suggested a model based on the Direct-Control Cycle for improving the quality of policies in information security governance. Jones and Rastogi (2004) discussed the importance of gaining improvements from software developers during the software developing phase in order to avoid security implications. Siponen et al. (2007) advanced a new model that explains employees' adherence to IS policies and found that threat appraisal, self-efficacy and response efficacy have an important effect on intention to comply with information security policies.

In terms of information security, behaviour is the perception of organizational norms and values associated with information security and so it exists within the organizations, not in the individual. To this end, individuals with different backgrounds or at different levels in the organization tend to describe the organization in similar way (Robbins, 1994). Security culture is used to describe how members perceive security within the organization. Since security and risk minimization are embedded into the organizational culture, all employees, managers and end-users must be concerned of security issues in their planning, managing and operational activities.

2.3 The issue of communication

Communication, in simple terms, can be considered as an interactive process of sending and receiving messages among individuals, groups, and organizations including some form of feedback. Although there are numerous definitions for the term "communication", this investigation adopts DeVito's (1988, p.14) definition that covers the essentials of the communication as the act: "*communication refers to the act, by one or more persons, of sending and receiving messages that are distorted by noise, occur within a context, have some effect, and provide some opportunity for feedback*".

However, risk communication is believed to be part of the risk management process as it allows the selection of risk control options and supplies the information on which third parties such as the government, industry or individual decision makers base their choices (National Research Council, 1989). Thus, the US National Research Council (NRC) defines risk communication as: *Risk communication is an interactive process of exchange of information and opinion among individuals, groups, and institutions. It involves multiple messages about the nature of risk and other messages, not strictly about risk, that express concerns, opinions, or reactions to risk messages or to legal and institutional arrangements for risk management* [NRC, p. 21].

However, risk communication is more complicated and difficult as it might appears. In particular, what makes risk communication difficult is not only the exchange of information amongst the parties involved, but also amongst the wider institutional and cultural contexts within which risk messages are formulated, transmuted and embedded (Krimsky and Plough, 1988).

The National Research Council distinguishes between two types of major problems in risk communication: those deriving from institutional and political systems and those between risk communicators and receivers. In the first case, various kinds of legal considerations such as liability and informed consent, affect the content of risk messages by influencing the available options for risk managers. Similarly, the problems between risk communicators and receivers arrive in case of difficulty to establish and recognize credibility, being alert in case of emergency, make messages understandable, capture and focus public's attention, and receive information (NRC, 1989).

Moreover, the success of risk communication is limited due to the insufficient attention it pays to social contexts within which individuals live and communicate (Otway and Wynne, 1989). In addition, it should be considered that the parties sending the messages may not always be honest, reliable as well as responsible (Otway and Wynne, 1989).

Risk communication though emerged from risk perception as the general public concerns about hazards were different to those of the experts, i.e., the scientific and policy making communities (NRC, 1989; Slovic, 1990). The difference, in particular, was that experts tended to focus on measurable, quantified attributes of risks while the public tended to focus on the qualitative value-laden attributes of risks such as fairness and controllability (Groth, 1991).

Sandman (1987) uses the term “outrage” to incorporate many of the qualitative dimensions of risks while “hazard” is the quantitative, measurable aspect of risk. According to him, although the public seems concerned with “outrage” at the expense of “hazard”, the experts often tend to ignore “outrage” at their own danger. He also points out that if the public’s legitimate concerns are not being addressed by the risk management process, the outrage level will be greater than when the public concerns are taken into consideration.

Thus, risk communication was developed as a way to communicate effectively the experts’ assessments of risks to the public so that the public would understand the real nature of risks and at the same time, to diminish the tension among parties with different perceptions of risks (Herriot and Firestone, 1983).

3. Survey of perceptions on communication

Three hundred and twenty seven (143 women and 184 men) employees of a large sized bank in Greece took part in the survey. The respondents ranged from junior staff to senior management and were between the ages of 22 and 65. They completed an anonymous survey questionnaire that was circulated personally by the principal researcher and consisted by 18 items. The questions were designed to solicit a response on the participant’s perception of security, the likelihood of communicating with others organizational norms and values and their trust of others in communicating efficiently security messages within the organization. Table 1, shows an example of questions.

For the communication behaviour based questions, respondents evaluated their likelihood of engaging in security related task behaviours (i.e., ‘…indicate the likelihood of engaging in each activity) on a five point rating scale raging from ‘Very likely’ (1) to Very unlikely’ (5). For the security perception questions, respondents rated their perception of the security presented by each risky behaviour (i.e., …indicate how risky you perceive each activity to be) on a five point scale ranging from ‘Very significant’ (1) to ‘Very insignificant’ (5).

For the likelihood in communicating efficiently security messages based questions, respondents rated their perception of the likelihood of other people in the organization communicating in activities (i.e., …your opinion what is the likelihood of people in the organization participating and communicating in the following activities) on a five point rating scale raging from ‘Very likely’ (1) to ‘Very unlikely’ (5).

The information in this report is based on the initial response of the three hundred and twenty seven participants. Using a variation of Cochran’s (1977) formula suggested by Israel (2002) to determine sample sizes necessary for given combinations of precision, confidence levels and variability, this survey should have a confidence level of 95% with a precision level of greater that ± 4%.

The main purpose of the survey was to find out mainly the following: What is the individual’s perception of security involved in relative activities? What are the individuals’ perception of the likelihood that others will communicate to certain organizational norms and values with regard to certain security activities? What are the individuals’ actual communication skills in understanding and circulating web security risk messages?

The intended outcome of this research is to develop a strategy to improve organizational information security and an enhancement of communication levels to managing efficiently security within the organizations. The questions analyze the different components relating to web banking security: 1) individual perception of web banking security, 2) individual perception of the likelihood that others will behave according to the organizational norms and values, 3) individual perception of communication in managing efficiently web banking security activities.

Table 2, shows the responses in percentages of the individual perception of security for certain web banking activities (perceived values), the individual perception of web banking security messages that others are determined to communicate efficiently in security task related activities (communication through information sharing), and the individual perception of behaving to organizational norms and values with regards to web banking security. The results give interesting insights and reveal gaps in the individual's perception of information web banking security and communication in the context of organizational norms and values. Male and female respondents don't differ significantly in their perceptions of web banking security in all activities with the exception of challenging another's knowledge on security related tasks where 62% of females perceived very significant risk in undertaking this activity. It would appear that generally female respondents are less likely to engage in risky behaviour. Surprisingly 38% of both male and female respondents perceive that it is likely or very likely that people within the organization are sharing passwords with other people. In addition, 84% of male and 78% of female respondents perceive it to be a significant risky activity. While 11% of male and 13% of female respondents implied that they would share a password with other people. Thus, it appears that while sharing passwords with others is considered risky with regards to web security, organizational norms and values ignore such behaviour.

In the context of others communicating efficiently security risk messages, 23% of male and 33% female respondents perceive hiding information from a co-employee as a risky activity yet 82% of male and 73% of female respondents said it was unlikely or very unlikely they would participate in the activity. This may imply that while individuals don't perceive this as a very risky activity, they intent to share information with others which means that the organization's norms and values enable cooperation and overall communication among the employees.

Of the total respondents 42% said that they would reuse the same password many times and in terms of web banking security project communication 53% said that they would ask for clarity of goal achievement in case they are confused. Finally, 53% said that project communication initiates from top-executives and that positive communication with top-management provides better understanding and control of security issues. In effect, communication is improved. The questionnaires were taken anonymously to enhance true value, although there is an uncertainty of answers that conform to what the security policy state with regards to web banking activities as well as the employee's actual behaviour.

15. In your opinion what is the likelihood of people in the organization to participate in the following activities: a) Share their passwords with other employees. b) Access files they are not authorized for. c) Try to "gain" others passwords without their permission.
16. For each of the following activities, please indicate how secure you perceive each activity to be: a) Share your password with another employee. b) Someone from outside the bank access the bank's internal network. c) Produce web security related manual for security incidents.
17. Please indicate your perception of others in communicating efficiently the following security related activities: a) Challenge another employee on security related tasks. b) Hide information from a co-workers from fear in keeping your "*work position*". c) Talk within the group about task related problems and try to solve them instantly.
For each of these activities, please indicate the likelihood of communicating with others organizational norms and values: a) Share a social incident within the group you belong to. b) Do not share your knowledge with others due to competitive reasons. c) Expect moral or money rewards for task related achievement.

Table 1. Example of Questions

All figures are shown as percentage (%)	**Male**	**Female**	**Male**	**Female**	**Male**	**Female**	**Male**	**Female**	**Male**	**Female**
Perception of security for these activities	Very Significant		Significant		Neutral		Insignificant		Very Insignificant	
Share password with others	50	47	34	31	14	14	12	10	7	5
Challenge new employee in work place	20	24	38	38	17	12	11	13	6	4
Allow another to use ID pass/card	38	47	33	32	16	16	21	19	7	3
View or download prohibited material	32	47	31	33	20	10	7	11	5	4
Forge someone's signature	26	34	45	39	19	6	5	9	3	6
Access unauthorised files	37	31	41	34	17	17	19	13	4	3
Challenge another's knowledge on security tasks	40	62	30	22	12	11	32	29	12	5
Hide information from other employees	19	21	22	19	12	14	12	21	11	12
Likelihood of communication in managing efficiently web banking security	**Very Likely**		**Likely**		**Neutral**		**Unlikely**		**Very Unlikely**	
Share password with others	18	21	22	19	12	13	29	30	21	22
Challenge new employee in work place	16	14	12	11	13	18	24	21	11	22
Allow another to use ID pass/card	6	7	3	10	17	13	33	21	19	21
View or download prohibited material	3	1	3	12	11	10	32	29	51	14
Forge someone's signature	1	1	2	6	5	3	33	21	59	26
Access unauthorised files	2	3	5	4	15	13	20	19	50	61
Challenge another's knowledge on security tasks	25	31	24	21	12	11	21	19	48	72
Hide information from other employees	21	20	19	24	11	19	34	25	29	26
Perception of the likelihood that others will communicate positively to organizational norms and values with regards to web banking security information sharing	**Very Likely**		**Likely**		**Neutral**		**Unlikely**		**Very Unlikely**	
Share password with others	6	4	7	9	11	14	21	18	49	50
Challenge new employee in work place	30	21	32	28	16	11	29	19	46	10
Allow another to use ID pass/card	7	3	3	2	17	12	23	18	33	30
View or download prohibited material	3	2	9	11	1	5	37	31	7	23
Forge someone's signature	4	1	8	2	1	6	11	9	43	56
Access unauthorised files	3	2	8	4	11	5	12	9	77	56
Challenge another's knowledge on security tasks	35	31	23	21	16	10	19	21	44	43
	32	29	31	28	17	22	33	41	49	32

Table 2. Security perception, perception of communication and likelihood ratings by gender

4. Limitations and further research

There are opportunities to undertake further intensive research to identify more critical behavioural and psychological factors and their relation in the context of web banking security. Although high levels of organizational norms and values sharing seems to positively affect communication on web banking security development and management, we cannot be sure as to how such results could always lead to an efficient web banking security management through information sharing. Future research on information systems and web banking security, especially research based on surveys, should therefore examine the role of other possible factors at the level of security planning and management. Likewise, another issue interesting to investigate would be the role and type of feedback in communication and organizational cultures in the context of web security design, e.g., whether the type of feedback (outcome or process feedback) provided affects the communication and web security management relationship.

However, there were some biases during the collection of data mainly due to the suspicious attitude of the IT employees towards the researchers. That is, the IT employees through the survey might be careful in answering questions with regards to security because the issue of information systems security is highly confidential and sensitive. To this end, open-ended questions were of useful to some extend.

Moreover, the research findings may be influenced by political games that different banking units wish to play. As the participation in a research survey can help organizational members to voice their concerns and express their views they can use this opportunity to put forward those views that they wish to present to other members of the organization.

5. Conclusions

There was a belief that web banking and security were difficult issues to be understood by non-IT staff. In recent years, it is believed that people make the difference to e-commerce based banking development activities and security management and that training on the ethical, legal and security aspects of information technology usage should be ongoing at all levels within organizations (Nolan, 2005). Since people react differently to poorly constructed security messages, communication will broken down and may confuse task knowledge and security risk awareness among the employees. Thus, the main implication for web banking security management is to focus on changing attitudes and human behaviour which are parts of the organizational norms and values in order to enhance awareness among the employees about information security related tasks. In doing so, efficient communication of security risk messages among end-users will increase since it is important to realize that awareness is one of the first steps to obtain active employee’s participation in the web banking security process and vice versa. That is, a well established security awareness will ensure web security project communication though active participation of employees to security related tasks.

The more organizations rely on information systems to survive in competitive markets, the more increasing becomes the need to maintain the confidentiality, availability, and integrity of data through the organization’s network and telecommunication channels. However, the technology advancement rate for the use and management of these information systems is more radical than the development of means for ensuring the confidentiality, availability, and integrity of data through them. That is, as organizations become aware of security issues, security threats remain high.

Although achieving the required level of web banking security requires also security awareness and control, a better understanding of the organization’s norms and values in which security measures are tailored to, is also important. In this way, organizations may have a clearer insight into how to communicate more efficiently to such security measures.

6. References

[1] Albrechtsen, E. 2007 A Qualitative Study of User’s View on Information Security, *Computer and Security*, 26(4), pp. 276-289.

[2] Boss, R.W. (1980) Trust and managerial problem solving revisited, *Group and Organization Studies*, 3(3), pp. 331-342.

[3] Burt, R.S., Gabbay, S.M., Holt, G., Moran, P. (1994) Contingent Organization as a Network Theory: The Culture-Performance Contingency Function, *Acta Sociologica*, 37(4), pp. 345-370.

[4] Coleman, J. (1990) Foundations of Social Theory, Cambridge, Harvard University Press.

[5] Computer Weekly (2009) UK small business not up to speed on security, Report.

[6] Davis, J., F.D. Schoorman, R., Mayer, H. Tan (2000) Trusted unit manager and business unit performance: Empirical evidence of a competitive advantage, *Strategic Management Journal*, 21(2), pp. 563-576.

[7] Debar, H. and Viinikka, J. 2006 Security Information Management as an Outsourced Service, *Computer Security*, 14(5), pp. 416-434.

[8] DeDreu, C., E. Giebels, E. Van de Vliert (1998) Social motives and trust in integrative negotiation: The disruptive effects of punitive capability, *Journal of Applies Psychology*, 83(3), pp. 408-423.

[9] DeVito, J.A. (1988) *Human Communication*, 4th edition, New York: Harper & Row, Inc. Dhillon, G. 2001 Challenges in managing information security in the new millennium. In: *Information security management: global challenges in the new millennium*, ed. Dhillon, G. USA: Idea Group Publishing, pp. 1-8.

[10] Dhillon, G. and Torkzadeh, G. 2006 Values-focused assessment of information system security in organizations, *Information Systems Journal*, 16(3), pp. 293-314.

[11] Ernst and Young (2008) Global Information Security Survey, Report.

[12] Gefen, D., Karahanna, E. and Straub, D. (2003) Trust and TAM in online Shopping: An Integrated Model, *MIS Quarterly*, 27(1), pp. 51-90.

[13] Gefen, D. and Straub, W. (2004) Consumer Trust in B2C e-Commerce and the Importance of Social Presence: Experiments in e-Products and e-Services, *Omega*, 32(6), pp. 407-424.

[14] Groth, E. (1991) Communicating with Consumers About Food Safety and Risk Issues, *Food Technology*, 45(5), pp. 248-253.

[15] Herriot, R. E., and Firestone, W. A. (1983). Multisite Qualitative Policy Research: Optimizing Description and Generalizability, *Educationa Researcher*, 12(3), pp. 14-19.

[16] Hwang, P., W. Burger (1997) Properties of trust: An analytical view, *Organizational Behavior and Human Decision Processes*, 69(1), pp. 67-73.

[17] Jones, R.L. and Rastogi, A. 2004 Secure Coding: Building Security into the Software Development Life Cycle, *Information Systems Security*, 13(5), pp. 29-39.

[18] Keeney, R.L. (1999) The Value of Internet Commerce to the Customer, *Management Science*, 45(3), pp. 533-542.

[19] Koskosas, I.V. (2008) Goal Setting and Trust in a Security Management Context, *Information Security Journal: A Global Perspective*, 17(3), pp. 151-161.

[20] Kotter, J.R. and Heskett, J.L. (1992) *Corporate Culture and Performance*, New York: Free Press

[21] Kramer, R.M. (1999) Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions, *Annual Reviews Psychology,* 50(1), pp. 569-598.

[22] Krimsky, S. and Plough, A. (1988*) Environmental Hazards: Communicating Risks as a Social Process*, Dover, MA: Auburn House Publishing.

[23] Larson, C., F. LaFasto (1989) Teamwork, Newbury Park, CA: Sage.

[24] Leach, J. 2003 Improving User Security Behaviour, *Computers and Security*, 22(8), pp. 685-692.

[25] Mayer, R.C., J.H. Davis, F.D. Schoorman (1995) An integrative model of organizational trust, *Academy of Management Review*, 20(1), pp. 709-734.

[26] McCumber, J. 2005 *Assessing and managing security risk in IT systems: a structured methodology*, USA: Addison- Wesley.

[27] McKnight, D.H., Cummings, L.L. and Chervany, N.L. (2002) Developing and Validating Trust Measures for E-Commerce: An Integrative Typology, *Information Systems Research*, 13(3), pp. 334-359.

[28] National Research Council (1989) *Improving Risk Communication*, Report of the Committee on Risk Perception and Communication, Commission on Behavioural and Social Sciences and Education, National Research Council. Washington, D.C.: National Academy Press.

[29] Nolan, J. 2005 Best practices for establishing an effective workplace policy for acceptable computer usage, *Information Systems Control Journal*, 6(2), pp. 32-35.

[30] Nootboom, B. (2002) Trust: Froms, Foundations, Functions, Failures and Figures, Edward Elgar Publishing Ltd, Cheltenham UK, Edward Elgar Publishing Inc, Massachusettes, USA.

[31] OECD- Organization for Economic Co-operation and Development (2002) Guidelines for the Security of Information Systems and Networks Towards a Culture of Security, report.

[32] Otway, H. and Wynne, B. (1989) Risk communication: Paradigm and Paradox, *Risk Analysis*, 9(2), pp. 141-145.

[33] Orlikowski, W. and Gash, D. (1994) Technological Frames: Making Sense of Information Technology in Organizations, *ACM Transactions on Information Systems*, 12(3), pp. 174-207.

[34] Putnam, L.L. (1993) The interpretive Perspective: An Alternative to Functionalism, Communication and Organization, L.L. Putnam and M.E. Pacanowsky, Beverly Hills, CA, Sage: 31-54.

[35] Quocirca (2009) Ignorance is not bliss, Report.

[36] Ridings, C., Gefen, D. and Arinze, B. (2002) Some Antecedents and Effects of Trust in Virtual Communities, *Journal of Strategic Information Systems*, 11(3/4), pp. 271-295.

[37] Robbins, S. 1994 *Management*, USA: Prentice-Hall Inc.Rousseau, D., Sitkin, S., Burt, R. Camerer, C. (1998) Not so different after all : A cross-discipline view of trust, *Academy of Management Review*, 23(3), pp. 387-392.

[38] Sandman, P. (1987) Risk Communication: Facing Public Outrage, *EPA Journal*, 13(9), pp. 21-22.

[39] Sarker, S., Valacich, S.J. and Sarker, S. (2003) Virtual Team Trust: Instrument Development and Validation in an IS Educational Environment, *Information Resources Management Journal*, 16(2), pp. 35-55.

[40] Sherwood, J., Clark, A. and Lynas, D. 2005 *Enterprise Security Architecture: A business- Driven Approach*, San Francisco, CA, USA: CMP Books.

[41] Simpson, B. and Wilson, M. (1999) Shared Cognition: Mapping Commonality and Individuality, *Advances in Qualitative Organizational Research*, 2, pp. 73-96.

[42] Siponen, M., Pahnila, S. and Mahmood, A. 2007 Employees' Adherence to Information Security Policies: An Empirical Study, In: IFIP International Federation for Information Processing, Vol. 232, *New Approaches for Security, Privacy and Trust in Complex Environments*, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J. von Solms, R., (Boston: Springer), pp. 133-144.

[43] Siponen, M. and Willison, R. (2007) *A Critical Assessment of IS Security Research Between 1990-2004*, The 15th European Conference on Information Systems, Session chair: Erhard Petzel, pp. 1551-1559.

[44] Souris, A., Patsos, D., and Gregoriadis, N. 2004 *Information Security*, ed. New Technologies, Athens, in Greek, First Edition.

[45] Straub, D. and Welke, R. (1998) Coping with Systems Risks: Security Planning Models for Management Decision Making, *MIS Quarterly*, 22(4), pp. 441-469.

[46] Workman, M. (2007) Gaining Access with Social Engineering: An Empirical Study of the Threat, *Information Systems Security*, 16(6), pp. 315-331.

[47] Von Solms, R. and Von Solms, S.H. 2006 Information Security Governance: A model based on the Direct-Control Cycle, *Computers and Security*, 25(6), pp. 408-412.