World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 3, 79-87, 2011

Internet Banking Security Management through Trust Management

Ioannis Koskosas
Department of Informatics and Telecommunications Engineering
University of Western Macedonia
KOZANI, Greece
ioanniskoskosas@yahoo.com

Maria-Mirela Koskosa
Department of Architecture and Visual Arts
University of East London
London, UK
mirelakoskosa@hotmail.com

Abstract— The aim of this research is to investigate information systems security in the context of security risk management. In doing so, it adopts a social and organizational approach by investigating the role and determinants of trust in the process of security goal setting with regard to internet banking risks. The research seeks to demonstrate the important role of trust in the risk management context from a goal setting point of view through a case study approach within three financial institutions in Greece. The determinants of trust are also explored and discussed as well as the different goal setting procedures within different information system groups. Ultimately, this research provides a discussion of an interpretive research approach with the study of trust and goal setting in the risk management context and its grounding within an interpretive epistemology.

Keywords- trust; goal setting; security management; internet banking; interpretive epistemology

I. INTRODUCTION

The research described in this article is concerned with information systems security in the scope of internet banking. Banking is being a highly intensive activity that relies heavily on information technology (IT) to acquire, process and deliver the information to all relevant users. To this end, IT provides a way for banks to differentiate their products and services delivered to their customers. Driven by the challenge to expand and capture a larger market share of the banking industry, some banks invest in bricks and mortar while others have considered a new approach to deliver their banking services via a new medium: the Internet.

While the internet provides opportunities for businesses to increase their customer base, reduce transactions costs, and sell their products globally, security implications impede the business [18]. As an example, a number of major studies recently conducted in Europe, among these being [1, 17, 14], indicate a general upward trend in the number of security incidents in organizations. These studies further suggest, that organizations expressed less confidence about future security issues, noting that security incidents are increasing both in terms of number and complexity

Although a number of significant, valuable approaches have been developed for the management of information systems security, they tend to offer narrow, technically oriented solutions and ignore the social aspects of risks and the informal structure of organizations [3, 40, 39]. In this research information systems security is viewed as the control of risks arising from unauthorized access to and possession of information. In the context of information systems, the asset under consideration is data and the main IS security foundations are the integrity, confidentiality and authenticity of such data [18].

Thus the main principle of this research is that even if information system managers and groups have available a variety of security risk management methods, tools and techniques, they may not make an efficient use of them in the process of risk management. In saying so, this research supports the view that security risks may arise due to a failure to obtain some or all of the goals that are relevant to the integrity, confidentiality and availability of information through the internet banking channel.

To this end, this research adopts a social and organizational approach to investigate information systems security within the scope of internet banking by exploring and describing the role and determinants of trust and goal setting procedures in risk management. In the following, the chosen research approach is being discussed as well as its appropriateness for the research objectives. Then, the issue of internet banking and the reasons for choosing such topic for investigation is being discussed and the theories of trust and goal setting are introduced. Ultimately, the research presents the empirical findings and concludes on the usefulness of an interpretive epistemology.

II. THE INVESTIGATION APPROACH

In this investigation, a qualitative research approach having philosophical foundations, mainly in interpretivism, was deemed the most appropriate. Reference [33] describes qualitative research as simply, research based upon words, rather than numbers. A more generalized, but appropriate definition is: "Qualitative research is multimethod in focus, involving an interpretive, naturalistic approach to its subject matter" [13]. This definition implies that qualitative researchers study things in their natural environment and understand events in terms of the meaning people assign to them and this is the strategy applied to this investigation. The term 'interpretivism' is defined as "Studies that assume that people create and associate their own subjective and intersubjective meanings (inductive process) as they interact (processual) with the world around them (contextual) [35].

Interpretivism was particularly useful when the results were being obtained. The respondents were providing their views from their interactions with the rest of the group in which goal setting was in process. For instance, when the respondents were asked questions regarding security goals, it was difficult for them to provide a response without having been involved in goal setting procedures.

The next issue under consideration was the research method to be used. Having considered the possible benefits of each available method e.g. action research, case studies, field studies, application descriptions, it was decided that the advantages offered by case studies were deemed more appropriate to this research. References [8, 47] cite a benefit of a case study as 'an investigation of a phenomenon within its real life context'.

However the question was whether to employ single case studies or multiple case studies. Theorists support the view that a single case study should be employed, particularly when exploring a previously unresearched subject [47] or for theory testing by confirming or refuting theory [31]. When a single case study is used, a phenomenon is investigated in depth, and a rich description and understanding are acquired [45].

Conversely, multiple case studies enable the researcher to relate differences in context to constants in process and outcome [8]. According to [33] multiple case studies can enhance generalisability, deeper understanding and explanation. Reference [22] point out that the evidence from multiple case studies is often considered more convincing, with the overall study being considered more robust. This investigation further asserts that although studying multiple cases may not provide the same rich descriptions as do studies of single cases, multiple cases enable the analysis of data across cases.

To this end, a case study approach has been followed within the IT departments of three financial institutions in Greece due to the investigator's availability of access. The institutions ranged from small (Alpha-Bank)1 to medium (Delta-Bank) to large (Omega-Bank) financial institutions accordingly, based on their financial assets. The reason for choosing these organizations according to their assets was to investigate the role and effect of trust on different goal setting procedures within different IT group structures. For example, the IT department of Alpha-Bank consisted of approximately 40 employees, while in Delta-Bank 150 employees, and in Omega-Bank 410 employees, respectively.

However, another issue to be resolved with the research approach used here concerns data collection. The design of this investigation employed multiple data collection methods as it is important in case research studies [5]. In all cases data was collected through a variety of methods including interviews, documents, and observation and visits to the banks lasted for approximately three months. The total number of interviews within the three case studies, numbered to fifteen. The interviewees ranged from IT managers, deputy managers, auditors, and IT staff people. The interviews were face-to-face and when necessary telephone interviews followed up to confirm something about the data that was unclear. In most cases, the conversations were tape-recorded. Tape recordings were used as they offer benefits that are not available with such other forms as the note taking of data collection.

Further, the use of multiple data collection methods makes triangulation possible and this provides stronger substantiation of theory [16]. Triangulation is not a tool or strategy, but rather an alternative to validation [13, 19]. Thus, any finding or conclusion made from the cases is likely to be more convincing and accurate if it is based on several different sources of information [47]. Five types of triangulation have been identified in the literature [24]: Data, Investigator, Theory, Methodological triangulation and Interdisciplinary. The present research used data triangulation, theory, methodological, and interdisciplinary. Having discussed the research approach, this investigation discusses the issue of internet banking and then introduces the theories of goal setting and trust.

III. THE INTERNET BANKING PHENOMENON

The internet has rapidly gained popularity as a potential medium for electronic commerce. The reason of such popularity is the fact that individuals have the ability to communicate and exchange information with people all over the world [21]. Firms have the potential to reach a large number of customers and fully automate their transactions in the values chain [25] while governments can provide more efficient services to citizens by automated procedures such as public procurement and local or national elections [2]. Today, the internet is believed to be on its way to become a full-fledged delivery and distribution channel while among the consumer-oriented applications riding at the forefront of this evolution are electronic financial products and services [41].

The emergence of internet banking has made banks re-think their IT strategies in order to remain competitive as internet banking services is believed to be crucial for the banks' long-term survival in the world of electronic commerce [7]. Today,

[1] The Three Case Studies in this article are described as Alpha-Bank, Delta-Bank, and Omega-Bank respectively, for confidentiality reasons

customers demand new levels of convenience and flexibility [27] on top of powerful and easy to use financial management tools, products and services, something that traditional retail banking could not offer [48]. Thus, internet banking allows banks to provide these services by exploiting an extensive public network infrastructure [42].

The use of new distribution channels such as the internet, however, increases the importance of security in information systems as these systems become sensitive to the environment and may leave organizations more vulnerable to system attacks. Thus, the issue of security in the context of internet banking is an interesting candidate to investigate.

IV. THE GOALS THEORY

The theory of goal setting falls within the broad domain of cognitive psychology and its literature is extensive. The theory, as the name implies, is based on the concept of goals and is an essential element of social learning theory [4], which has become increasingly influential through time [34]. Goals, however, can be viewed as internal psychological representations of desired states, which can be defined as outcomes, events, or processes [34]. A goal encompasses terms such as intention, aim, task, deadline, purpose and objective. It is part of the human condition, in the sense that almost all human activities are consciously or unconsciously directed by goals.

The importance of goals with respect to work behavior is well documented by two main propositions, these are:

- Increases in the difficulty of assigned goals (given goal acceptance) lead to increases in performance
- Specific, difficult assigned goals result into higher performance than instructions of 'do your best' or no assigned goals.

In the first proposition, research shows that when individuals accept an assigned difficult goal, task performance tends to increase. In particular, 90 percent of the studies support this proposition with an effect size on performance being approximately 10-15 percent increase as a result of goal level [29]. Likewise, in the second proposition research shows that when individuals are given goal specificity, task performance tends also to increase. Based on the same research findings, [29] report that 90 percent of those studies support the second proposition with an effect size on performance being approximately 8-16 percent increase as a result of goal specificity.

Some recent research results though show that the relationship between goal level- performances may not necessarily hold at a macro (group) level. For instance, [49] found different impacts of goal setting on performance based on group size, while [46] found moderating effects from participation in goal setting, group cohesion and group conflict. The majority of the results though show that the two propositions hold for both individual and group levels in laboratory and field studies as well as in different types of tasks.

Following these trends, this investigation takes a macro-goal level point of view and supports that an efficient goal setting process, at group level, will improve the process of information systems risk management within the scope of internet banking security. Thus, the main research question becomes:

- Do organizations set goals relevant to the management of the integrity, confidentiality and availability of information through the internet banking channel?

V. THE TRUST THEORY

Trust is a social phenomenon. In their research [36] review several studies [20, 9, 37] on trust. These studies argue that trust determines the performance of a society's institutions so that according to them trust is a propensity of people in a society to co-operate to produce socially efficient outcomes [9]. Reference [37], for example, defines trust as a habit formed over centuries' long history of "horizontal networks of association" between people covering both commercial and social activities. Reference [38, p. 395] defined trust as: a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another. In this investigation, we treat trust as one dimension psychological state, although we recognize that trust is a complex psychological state that may consist of different dimensions.

A handful of studies suggest that trust is beneficial to organizations through two main effects. Either when trust results in direct effects on a variety of outcomes or when moderates the effects of other determinants on attitudinal, perceptual, behavioral, and performance outcomes via two distinct perceptual processes. Hence, instead of proposing that trust directly results in desirable outcomes, this investigation suggests that trust moderates the effects by providing the conditions under which there will be a certain effect on goal setting procedures. In doing so, trust is defined as confidence and positive expectations of one work partner within an IT group that another work partner is willing to co-operate to set goals efficiently in the context of internet banking security.

According to [32], individuals' beliefs about another's ability, benevolence and integrity, lead to willingness to risk, which in turn leads to risk-taking in a relationship, as manifested in a variety of behaviors. Thus, a higher level of trust in a work partner increases the likelihood that one will take a risk with a partner (e.g., cooperate, share information) and/or increases in the amount of risk that is assumed. Consequently, risk-taking behavior is expected to lead to positive outcomes e.g. individual performance, and in social units such as work groups, cooperation, information sharing are expected to lead to higher unit or group performance [26, 28, 10].

However other studies examining the main effect of trust on workplace behaviors and outcomes found only partial support or no support. That is, while some studies report a significant main effect, others do not. For instance, while [6] found that trust within group has a positive effect on openness in communication, [11] found that trust between negotiators

mediates the effects of social motives and punitive capability on information exchange. Reference [23] proposed that trust is necessary, but not sufficient, condition for cooperation. This terminology suggests that trust may act as a moderator, although the mathematical model does not specifically consider how trust might operate in this manner.

Based on these literature findings on trust, this investigation further supports that trust may have an effect on the level of goal setting with regard to internet banking security. To this end, the investigation further supports that trust at group (macro) level:

- Plays an important role and has an effect on the process of goal setting with regard to internet banking security goals

TABLE 1. GOAL SETTING IN THE CONTEXT OF SECURITY RISK MANAGEMENT

1st Phase: Goal Setting Initiation Phase
Step 1: Selection of members for the project group
Step 2: Explanation of the method to the members of the group and planning of the goal setting security risk activities
Step 3: Physical security goals (external)
Step 4: Systems security goals (internal)
2nd Phase: Goal Execution Phase
Step 1: Risk identification goals
Step 2: Selection of identified risks
Step 3: Final risk identification and further goal setting via a joint security project group meeting
Step 4: Control of goal setting activities
Step 5: Risk monitoring
3rd Phase: Evaluation Phase
Last step: Evaluation of security risk go al setting activities and compiling a report
al setting activities and compiling a report

VI. RESEARCH FINDINGS

A. Goal Procedures

It was imperative for this investigation that any organization used for the research should have followed goal setting procedures and particularly the organizations' IT groups. Before the interviews commence the contacted organizations replied positively that goal setting was a consistent part of their overall business strategy. In fact, goal setting was a very important issue and it was seen as an integral part of the overall risk management process. All the interviewees within Delta and Omega-Bank stated that goals are being set on a regular basis within each banking unit respectively, and that goals represent the identity of the banks' business activities plan. The goals within both organizations, like in the case of Alpha-Bank, are always business oriented and within the technology units the main goals are cost reduction, automation of processes, systems efficiency, and security. Likewise, goals within the three organizations may come in the form of projects which either originates from the top-management to the different banking units or from those units to the top-management in the form of project proposals. Goal setting activities, in the context of risk management, are distinguished into three main phases, as shown in Table 1: the goal setting initiation phase, the goal execution phase, and the evaluation phase.

However it is not in the scope of this investigation to describe in detail each step of the goal setting phases within the organizations but rather to give an overall view of how the selected organizations set security goals. In saying so, the IT group within Delta-Bank distinguishes the monitoring phase into an independent phase instead of being part of the execution phase, like in the cases of Alpha- and Omega-Banks. Similarly, the first four steps at the goal initiation phase within the organizations were identical although the IT group at Omega-Bank considers the level of security applications in internet banking and alternative networks as separate levels of security goal activities. The interviewees within Omega-Bank argued that the additional taxonomy of security levels gives a more clear insight into the different aspects of security.

At the goal execution phase, all of the organizations exhibited similar patterns although at Delta-Bank the risk monitoring stage was assumed as an independent final phase from that of execution. Alpha-Bank, had also an additional step of controlling the goal activities planned, while Delta-Bank and Omega-Bank did not. At Alpha-Bank though this stage is considered as reactive since the IT group seeks feedback to ensure that the security goal setting plan until that stage, will actually accomplish its objectives. From the interviews, Delta- and Omega-Bank considered that such feedback is achieved at the evaluation phase while at Alpha-Bank the IT group members argued that although feedback is achieved at the evaluation phase, some of the goal activities planned may be 'jeopardised' before that phase. Thus, the control of goal setting activities planned is a 'premature' stage, which provides though more valuable information at the time needed. In the context of internet banking security, all of the three case studies make use of a checklist which prioritises internet banking risks in terms of their likelihood ratio and possible impact. In doing so, the IT groups can take measures if necessary in order to maintain control of security related activities to internet banking.

Although, it was stated that the taxonomy of such risks and risk factors in internet banking change on a regular basis, the provision of such a checklist was not provided due to confidentiality reasons. However, in the case of Alpha-Bank, an example of such checklist was obtained for the purposes of this investigation. This checklist is included in Appendix 1, which consists of five main clusters of internet banking risk categories.

The evaluation phase was also a significant stage of the overall goal setting process in the context of security risk management within all of the three IT groups. In the case of Omega-Bank, however, the IT group considered an additional activities step, that of security policies and procedures, based on which the IT group investigates whether there is a need to change any particular aspect. The difference in the case of

Omega-Bank, as compared to the case of Alpha-Bank and Delta-Bank, is that the IT group makes a more frequent evaluation of the security policies and procedures after the implementation of security projects.

However, goal setting within the three case studies was a significant and consistent part of the overall organizations' business activities plan and development. The procedures according to which the IT groups within the three organizations set goals, in the context of risk management, exhibit similar patterns although with a few minor differences in the implementation process, in terms of stage prioritization. In the context of internet banking security, all of the interview respondents within the organizations suggested that the use of the checklist proved to be beneficial as it provides clarity of the internet banking risks and of the security goal activities that have to be planned.

TABLE 2. THE DETERMINANTS OF TRUST IN THE GOAL SETTING CONTEXT

▪ Time ▪ Clarity and stability in decision making ▪ Participation in decision making and group activities ▪ Job satisfaction ▪ Moral rewards (promotions, performance evaluations, guidance on job responsibilities, training) ▪ Money rewards ▪ Group solidarity ▪ Role guidance ▪ Downsizing

B. The Role and Effect of Trust on Goal Procedures

As previously described, goal setting within Delta- and Omega-Bank was an integral part of the organizations' overall business activities plan. From the interviews within Delta-Bank, the issue of trust was believed to have an effect on the level of goal setting to the degree that one party or group was capable of delivering. The differences of the business scope within different banking units had an effect on the IT groups' activities because the business units did not seek always to 'deliver'. Thus, some of the IT projects found difficulties at the project initiation phase, as the IT groups had to postpone decisions on security issues. Such an example includes the upgrade of the system fault tolerance level and the issue of vulnerability assessment.

The restriction imposed to some IT employees to participate in the process of goal setting with regards to the security of internet banking, established a level of mistrust between these employees to the management, as they felt incapable of delivering. To this end, considering that trust in this investigation has been defined as willingness to co-operate in order to produce efficient work outcomes, trust had an effect on the level of security goal setting, although weak, as the non-participation of some IT employees to goal setting did not allow them to co-operate efficiently and even transfer their knowledge to other members within the group.

Similar patterns were exhibited in the case of Omega-Bank with the establishment of the Disaster Recovery Planning (DRP) centre, whereas different stakeholders' interests were diverged from those in the IT group. In effect, the DRP's input to goal setting was controlled since the DRP activities contribute to the risk monitoring and evaluation phase, as they also focus on post-evaluation implementation on security related projects.

C. The Determinants of Trust on Goal Procedures

The investigation proceeded further to the identification of the determinants of trust within all of the three organizations. The findings are based on the interviewees' work related experience, social relationships between people within groups, knowledge, and personal value attributes.

One of the first determinants of trust mentioned in the interviews, is time. As stated, trust develops over time through transparent relationships between the members of either an organization or group, although trust is easy to loose. All the interviewees commonly agreed that trust depends on past performance of a group or individual and it builds upon time. They also stated that the manager of the IT group in particular, is responsible for exhibiting 'healthy' patterns of trust in terms that the decisions he makes do not cancel each other out, continuously. For example, in Alpha-Bank it was mentioned that if the IT manager categorizes the group's activities to specific individuals and then, he changes his mind and rearranges the individuals' responsibilities in the group, those individuals not only will be confused but also they will lose trust to the manager, in terms of being capable to make decisions.

Participation in decision making and in group activities is also another determinant of trust, since the IT employees feel that they can contribute to the group and that their input is being appreciated. Job satisfaction is also important, which means that if the employee likes the nature of his job and job related responsibilities he will be more likely to trust his manager and willing to co-operate in order to produce efficient work outcomes. Similarly, all of the interviewees within the three case studies stated that moral and money rewards are also important determinants of trust. In the context of moral rewards, the manager plays a significant role in establishing trust among his employees since he is responsible for many duties such as performance evaluations, promotions, guidance on job responsibilities, and training. Money rewards is perhaps the most important determinant of trust, particularly in organizations where trust is viewed in terms of professionalism, such as Delta- and Omega-Bank, respectively. The respondents in Delta and Omega-Bank said that having money incentives creates a feeling of trust towards the top-management, as the employees' contribution is rewarded.

During the interviews within the case of Alpha-Bank, the people also stated that group solidarity is another determinant of trust, in terms that different members within the group have to equally share the responsibilities assigned by the manager. In addition, they mentioned that each member has to understand his role within the group, something of which responsible is also the group's manager. Downsizing is also an important determinant of trust because during organizational downsizing survivors sense of empowerment can decrease and survivors do not believe that top-management communication is credible or

that information is being withheld [31]. All these determinants are exhibited in Table 2 below.

D. Limitations and Further Research

There are opportunities to undertake further intensive research to identify more social and organizational factors that affect communication standards and procedures in internet banking security management. Although high trust levels seem to positively influence internet banking security, we cannot be sure as to how trust can always do that. Future research should focus on the perception and development of trust development strategies and how they could be applied to different organizational structures as well as security measures and policies according to organizational structure size that improve employees awareness on internet banking security issues. That said, different structured organizations may have different business objectives and therefore, security needs. Likewise, another issue interesting to investigate would be the role and type of feedback in trust relationships in the context of internet banking, e.g., whether the type of feedback (outcome or process feedback) provided affects the trust-information security relationship.

The relationship between theory and practice may be considered weak and unstructured, as qualitative approaches have been criticised for not infusing theoretical factors. To this end, in this investigation an attempt was made to address this issue by investigating the role and determinants of trust to the success of internet banking security. Although, qualitative research does not offer the pretence of replication since controlling the research will destroy the interaction of variables, this investigation was conducted in a structured methodology guided by the specific organizational factors based on the literature review.

Moreover, the research findings may be influenced by political games that different banking units wish to play. As the participation in a research study 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. To this end, in order to mitigate or record the effect of 'suspicion' for interpretive research, this investigation used a collection of various perspectives such as archival documents, reports, white papers, bank regulations and an interpretation of how the interviewees react to the opinion expressed by other members.

VII. CONCLUSIONS

The cases of Delta- and Omega-Bank exhibited slightly different patterns of socio-organizational behavior although the process of goal setting in the context of risk management was based on the same principles among the three case studies. Specifically, the undertaking of the three empirical studies revealed that IT managers and groups do set security goals with regard to the management of the integrity, confidentiality and availability of information through the internet banking channel. Moreover, evidence has shown that there is indeed an effect of trust on the level of security goal setting. However, this effect is stronger in organizations with small structures because such organizations exhibit 'family-oriented' business patterns whereas the values and beliefs are strongly held and widely shared among the organizational members. Although, the effect of such social and organizational issue applies to organizations with large structures, their impact is rather minimal because such organizations depend strictly on manuals and procedures, which focus on professional criteria rather than individual initiative and intellect.

Likewise the existence of different political agendas was found to have a greater impact to large organizations as compared to small ones. The conflict type identified within the three case studies was mainly due to differences in business scope between different banking units rather than due to insufficient knowledge on subject matters. The case of Alpha-Bank, the small structure organization, has exhibited greater flexibility in decision making and consistency within the IT group activities as compared to the other cases with large structures.

A major conclusion with regard to security is that social and organizational issues such as trust play an important role in the process of goal setting. To this end, failure to recognize and improve such socio-organizational issues may lead to inefficient processes of goal setting, whereas security risks with regard to the integrity, confidentiality, and availability of information through the internet banking channel, may arise.

Ultimately, this paper has made an important contribution to interpretive research by exploring and making practical recommendations for the process of goal setting within an interpretive research methodology. In particular, this investigation concludes that a social organizational approach is not independent of epistemological assumptions. In the opposite, this investigation has reinforced the argument that trust and goal setting are interrelated and that these aspects may have an effect in the context of information systems security management. In this respect, the research has contributed to a more holistic consideration of social organizational issues of information systems security as it allowed to break away from the narrow-technically oriented solutions of most IS security approaches to a variety of social, organizational issues that are of concern to researchers and practitioners alike.

APPENDIX 1: Internet Banking Security Checklist *(Alpha-Bank)*

VIII. CLUSTER 1: INTERNET BANKING POLICY

- **Internet banking risks and controls**
- **Transaction risks**
- **Control and security**
  Security controls
  Network and data access controls
  User authentication
  Firewalls
  Encryption
  Transaction verification
  Virus protection
- **Monitoring**

Security monitoring
Penetration testing
Intrusion detection
Performance monitoring
Audit/quality assurance
Contingency planning/business continuity
Internet expertise
Selection of internet banking providers
Internet banking functions available

IX. CLUSTER 2: INTERNET BANKING AND PHYSICAL SECURITY RISKS

- **Risk management and risk management controls**
  Security risks
  Costs versus security breaches
- **Controlling client PCs**
  Desktop computer controls
- **Password management**
  Password management alternatives
  Retrieving lost passwords
- **Watching the employees**
  Surveillance in and around the office
- **Controlling networks and servers**
  Managing network administration
  EFT switches and network services
  Electronic imaging systems
  Operational and administrative security
  Authentication security
  Encryption security
- **Shutting down compromised systems**
  Manageable security enforcement
  Sample secure applications e-mail security
  Internet access security
- **Physical security**
  Security monitoring system overview
  Major hazards
  Fire flooding
  Riot and sabotage
  Freud or theft
  Power failure
  Equipment failure
  Housekeeping rules

X. CLUSTER 3: INTERNET BANKING AUDITING

- **Website and internet banking features checklists**
  Website development and hosting
  Internet banking package
  Cash management package
  Bill pay
  Security
  Options
- **Internet banking policy**
  Goals and objectives
  Vendor management
  Maintaining the institution's image
  Insurance coverage
  User access devices
  File update responsibilities
  Account reconciliation
  Bill payment services
  Bill pay controls
  Bill pay processing
  Bill pay customer support
  Disaster recovery
  Employee access
  Security
  Internet banking services request/fulfillment
  Internet banking registration form
  User logs and error reports
  Privacy external links
  Dial-in access (if applicable)
  Audit
  Geographic boundaries

XI. CLUSTER 4: IDENTIFYING CUSTOMERS IN AN ELECTRONIC ENVIRONMENT

- **Establishing the identity of an applicant**
  Identification documents
  Information collection
  Verifying identification information
- **Assisting customers who are victims of identity theft**
  What to tell to victims of identity theft
  Using the FTCs affidarit
- **Authentication in electronic banking environment**
  Risk assessment
  Account origination and customer verification
  Transaction initiation and authentication of established customers
  Monitoring and reporting
  Authentication methods: passwords and PINs
  Digital certificates using public key infrastructures (PKI)
  Tokens
  Biometrics

V. CLUSTER 5: ELECTRONIC COMMERCE

- **The computer network**
  Security of internal networks
  Security of public networks
- **Electronic capabilities**
  Examination categories for electronic capabilities
  (Level 1: information only systems)
  (Level 2: electronic information transfer systems)
  (Level3: fully transactional information systems)
  electronic payment systems
  financial institution roles in electronic payment

systems

- **Risks**
  Specific risks to electronic systems
- **Risk management**
  Strategic planning and feasibility analysis
  Incidence response and preparedness
  Internal routines and controls
  Other considerations

REFERENCES

[1] Andersen, I.T. Security Barometer survey: The Psychology of Security, Quocirca, 2006.

[2] Andersen, K.V. EDI and Data Networking in the Public Sector: Governmental Action, Diffusion, and Impacts, Kluwer Academic Publishers, Boston, 1998.

[3] Backhouse, J. and Dhillon, G. Structures of Responsibility and Security of Information Systems, *European Journal of Information Systems*, 5(1), pp.2-9, 1996.

[4] Bandura, A. Self-efficacy: The Exercise of Control, New York, W.H. Freeman Publishing, 1997.

[5] Benbasat, I., Goldstein, D.K., and Mead, M. The Case Research Strategy in Studies of Information Systems, *MIS Quarterly*, 11(3), pp. 369-386, 1987 .

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

[7] Burnham, B. The Internet's Impact on Retail Banking, Booz-Allen Hamilton Third Quarter, (http://www.strategy-business.com/briefs/96301), 1996.

[8] Cavaye, A.L. Case Study Research: A Multi-Faceted Research Approach for IS, *Information Systems Journal*, 6(3), pp.227-242, 1996.

[9] Coleman, J. Foundations of Social Theory, Cambridge, Harvard University Press, 1990.

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

[11] De Dreu, C., E. Giebels, E. Van de Vliert. Social motives and trust in integrative negotiation: The disruptive effects of punitive capability, *Journal of Applied Psychology*, 83, 408-423, 1998.

[12] Denzin, N.K. The Research Act, Third Edition, Prentice-Hall, Eaglewood Cliffs, New Jersey, USA, 1989.

[13] Denzin, N. and Lincoln, Y. Major Paradigms and Perspectives, In: Strategies of Qualitative Inquiry, N.Y.K. Denzin and Y.S. Lincoln, (eds.) Sage Publication, Thousand Oaks, 1998.

[14] D.T.I. Security Special Report: The Internal Threat 2006, Technical Report, April, Department of Trade and Industry, London, 2006.

[15] DeVito, J.A. Human Communication, 4th edition, New York: Harper & Row, Inc, 1988.

[16] Eisenhardt, K. M. Building Theories from Case Study Research, *Academy of Management Review*, 14(4), pp.532-550, 1989.

[17] Ernest and Young Global Information Security Survey, Ernst & Young, London, 2006.

[18] Forcht, K. and Wex, R. Doing Business on the Internet: Marketing and Security Aspects, *Information Management and Computer Security*, 4(4), pp.3-9, 1996.

[19] Flick, U. Triangulation Revisited: Strategy of Validation or Alternative? *Journal for the Theory of Social Behaviour*, 22, pp. 175-198, 1992.

[20] Gambetta, D. Trust: Making and Breaking Cooperative Relations, Cambridge, UK, Basil Blackwell, 1998.

[21] Gore, A. Putting People First in the Information Age, In: Masters of the Wired World, A. Lee, eds., Financial Times Pitman Publishing, London, pp.31-36, 1999.

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

[23] Hwang, P., W. Burgers, Properties of trust: An analytical view, *Organizational Bahaviour and Human Decision Processes*, 69, 67-73, 1997.

[24] Janesick, V. The Choreography of Qualitative Research Design. In: Denzin, N.K. and Lincoln, Y.S. (eds.) Handbook of Qualitative Research. Thousand Oaks, CA: Sage, 2000.

[25] Kosiur, D. Understanding Electronic Commerce, Microsoft press, Redmond, Wash, 1997.

[26] Klimoski, R.J., Karol, B. The Impact of Trust on Creative Problem Solving Groups, *Journal of Psychology*, 61, pp.630-633, 1976.

[27] Lagoutte, V. The Direct Banking Challenge,Unpublished Honours Thesis, Middlesex University, 1996.

[28] Larson, C., F. LaFasto, Teamwork. Newbury Park, CA: Sage, 1989

[29] Locke, E.A. and Latham, G.P. A Theory of Goal Setting and Task Performance, Englewood Cliffs, NJ: Prentice-Hall, 1990.

[30] March, J.G. Exploration and Exploitation in Organizational Learning, *Organization Science*, 2(1), pp. 71-87, 1991.

[31] Markus, M.L. Case Selection in a Disconfirmatory Case Study, In: *The Information Systems Research Challenge*, Harvard Business School Research Colloquium, Boston: Harvard Business School, pp. 20- 26, 1989.

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

[33] Miles, M.B. and Huberman, A.M. Qualitative Data Analysis: An Expanded Sourcebook, Sage publications, Newbury Park, CA, 1994.

[34] Mitchell, T.R., Kenneth, R.T. and George-Falvy, J. Goal Setting: Theory and Practice, In: Industrial and Organizational Psychology: linking theory with practice, Editors: C.L. Cooper and E.A. Locke, Blackwell Publishers Ltd, First Published, 2000.

[35] Orlikowski, W. and Baroudi, J.J. Studying Information Technology in Organizations: Research Approaches and Assumptions, *Information Systems Research*, 2(1), pp.1-28, 1991.

[36] Porta, R., F. Lopez-de-Silanes, et al., Trust in Large Organizations, NBER working paper, 1996.

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

[38] Rousseau, D., Sitkin, S., Burt, R., Camerer, C., Not so different after all: A cross-discipline view of trust, *Academy of Management Review*, 23, pp. 387-392, 1998.

[39] Siponen, M.T., A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, 8(1), pp.31-41, 2000.

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

[41] Tan, M. and Teo, T.S.H. Factors Influencing the Adoption of Internet Banking, *Journal of the Association for Information Systems*, 1(5), July, 2000.

[42] Ternullo, G. Banking on the Internet: New Technologies, New Opportunities and New Risks, Boston Regional Outlook, Second Quarter, (http://www.fdic.gov/index.html), 1997.

[43] Tushman, M.L., and O' Reilly, C.A. III Winning through Innovation, Boston: Harvard School Press, 1997.

[44] U.S. Department of Commerce, The Emerging Digital Economy II, (http://www.ecommerce.gov/ede/), 1999.

[45] Walsham, G., Interpretive Case Studies in IS Research: Nature and Method, *European Journal of Information Systems*, 4(2), pp.74-81, 1995.

[46] Wegge, J., Participation in Group Goal Setting: Some Novel Findings and a Comprehensive Model as a New Ending Ton at Old Story, *Applied Psychology: in International Review*, 49(3), pp. 498-516, 2000.

[47] Yin, R.K., Case Study Research, Design and Methods, Sage Publications, Newbury Park, CA, 1984.

[48] Krimsky, S. Plough, O., Environmental Hazards: communicating risks as a social process. Auburn House, 1988.

[49] Latham, G. P., and Seijts, G. H., The effects of proximal and distal, *Organizational Behavior and Human Decision Processes*, 43, pp. 270 –287, 1999.

AUTHORS PROFILE

Dr. Ioannis V. Koskosas is a Senior Lecturer at the Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Greece as well as at the Technological Educational Institute of Western Macedonia, Greece. He teaches in the post-graduate program, the modules of information systems and network security and techniques of expression and communication. He specializes in information systems security, organizational issues and e-banking. Dr. Koskosas holds a Bachelor of Arts (BA) in Economics, a Masters of Science (BSc) in Money, Banking and Finance both from Middlesex University, London and a Doctorate of Philosophy (PhD) in Information Systems Security Management in e-banking from the School of Information Systems, Computing and Mathematics from Brunel University, London. He can be reached at ioanniskoskosas@yahoo.com.

Maria-Mirela Koskosa holds a BA (hons) in Architecture from Greenwich University, London, UK.