Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2010 Proceedings

Mediterranean Conference on Information Systems (MCIS)

9-2010

PRELIMINARY SURVEY RESULTS ON IT SECURITY PRACTICES IN CYPRUS PRIVATE AND PUBLIC SECTORS

Ionna Dionysiou
University of Nicosia, Cyprus, dionysiou.i@unic.ac.cy

Angelika Kokkinaki
University of Nicosia, Cyprus, kokkinaki.a@unic.ac.cy

Skevi Magirou
University of Nicosia, Cyprus, SMagirou@memrb.com.cy

Follow this and additional works at: http://aisel.aisnet.org/mcis2010

Recommended Citation

Dionysiou, Ionna; Kokkinaki, Angelika; and Magirou, Skevi, "PRELIMINARY SURVEY RESULTS ON IT SECURITY PRACTICES IN CYPRUS PRIVATE AND PUBLIC SECTORS" (2010). *MCIS 2010 Proceedings*. 25.
http://aisel.aisnet.org/mcis2010/25

This material is brought to you by the Mediterranean Conference on Information Systems (MCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MCIS 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

PRELIMINARY SURVEY RESULTS ON IT SECURITY PRACTICES IN CYPRUS PRIVATE AND PUBLIC SECTORS

Ioanna Dionysiou, dionysiou.i@unic.ac.cy

Angelika Kokkinaki, kokkinaki.a@unic.ac.cy

Skevi Magirou, SMagirou@memrb.com.cy

University of Nicosia, Cyprus

Abstract

This paper discusses users' practices on IT security in Cyprus organizations. This investigation is part of a broader research effort initiated by researchers at University of Nicosia that aims in the development of an enterprise Mashup application that private and public organizations could use to specify and manage their strategies regarding ICT security.

The questionnaire was drafted based on the IT Security Guidelines promoted by the national security agency of the German federal government, as it is a comprehensive checklist on security matters. A survey is currently underway among Cypriot organizations and enterprises regarding established security procedures and policies on ICT security. Based on the received responses (approximately half the expected sample size), preliminary results show that security mechanisms and their management are deployed in a majority of the organizations. A more accurate and complete analysis will be available upon completion of the survey.

Keywords: IT Security, Security Safeguards, Enterprise Mashup Security Application

1 INTRODUCTION

Currently, Information and Communications Technology (ICT) is transcending almost all aspects of life. Increased vulnerability and the threat of massive financial damage due to ICT malfunctions are augmenting the pressure to prevent damage and minimize the risk through active IT security management. However, ICT security strategies are perceived to require high investment in security technology while their implementation is also considered to be demanding in terms of highly skilled human resources. In view of these, security is not usually assigned high priority by organizations. This is even more pronounced for small and medium size enterprises (SMEs) due to various reasons including increasing complexity of ICT, lack of resources and increased financial investments, which becomes a significant burden in current economic crisis.

It has been noted that many organizations in Cyprus place at a relatively low priority initiatives related to ICT security. However, design and implementation of an effective ICT security concept need not necessarily be expensive. The main success factor is well thought out organizational procedures and reliable, informed staff who observe security requirements in a disciplined manner. Needless to say, in order to address ICT security concerns at the workplace, one has to uncover existing IT security strategies and policies. This paper discusses the preliminary results on ICT security practices in Cyprus private and public sectors based on a nationwide survey initiated by two research centers at University of Nicosia, the University of Nicosia Research Foundation (UNRF) and the Cyprus Academic Research Institute (CARI). The investigation is part of a broader research effort that envisions the development and deployment of an open-source application that would assist SMEs with limited financial and personnel resources implement security policy based on the particularities of their own environment.

The remaining of the paper is organized as follows: Section 2 discusses the SME Mashup IT security application, which is the ultimate goal of the research project. Section 3 describes the survey logistics on preparing the questionnaire on user security perceptions, followed by analysis of the responses. Section 4 concludes with future directions.

2 SME MASHUP IT SECURITY APPLICATION

An Enterprise Mashup may be defined as a "*Web-based resource that combines existing content, data or applications, from one or more providers by empowering the actual end users to create and adapt individual information centric and situational applications*" (Hoyer et al. 2008). Enterprise Mashup applications combine simplified concepts of Service-Oriented Architecture (SOA) with the principle of peer production (Daniel et al. 2007). The relevant architectural components of the Enterprise Mashup paradigm are Resources, Widgets, and Mashup applications (Hoyer et al. 2009). Resources may be content, data or application functionality and they are encapsulated via well-defined public interfaces (i.e., WSDL, RSS, Atom). The layer above contains widgets, which provide simple user interaction mechanism abstracting from the complexity of the underlying resources. Widgets are developed by consultants or key users in the business units who understand the business requirements and know basic development concepts. Finally, end users with no programming skills are able to combine and configure such visual widgets according to their individual needs, which results in an Enterprise Mashup.

Maximilien et al. (2008), Yu et al. (2008), Hoyer et al. (2008) refer to existing research efforts that focus on developments tools i.e., (IBM Mashup Center, Intel Mash Maker, Microsoft Popfy, and Kapow Mashup Server) and underlying technical concepts and principles. The discussion from a collaborative and peer production perspective is still missing in the scientific community discussing the implications, challenges, but also the potential benefits and limitations of the Mashup paradigm in the enterprise context, at large. In particular with respect to the involvement of end-users in ICT security safeguarding, researchers and practitioners (Bagchi and Udo 2003; Baskerville 1993; Dhillon and Backhouse 2000; Liang and Xue 2009, Loch et al. 1992; Stafford and Urbaczewski 2004; Straub and Welke 1998) have proposed models for user involvement and practices of excellence to prevent potential harm and losses from ICT security bridge. From this perspective, important questions are: who is involved in ICT security management, what are the roles of the different stakeholders, in particular of the ICT administrators and end-users in the various business units, what are procedures to be followed for ICT safety, how compliance with procedures is ensured, what are the contingency plans and what are the necessary processes to enable and sustain users community building and collaboration?

A research project, currently underway at University of Nicosia, aims to design and develop an Enterprise Mashup application that uses expert knowledge on ICT security (in the form of rules and ontology), a comprehensive repository in terms of relevant data (instances), and an interactive Human Computer Interaction (HCI) artifact through which custom ICT strategies are developed for interested organizations. Furthermore, the system will provide to visitors a constantly updated stream of relevant information and it will enable them to remain on top of the latest developments.

Methodologically, the first stage will involve elicitation of current IT security practices through a survey among involved stakeholders. Based on the user feedback, an HCI artifact will be designed in a way that will facilitate a user-friendly, efficient and effective experience. An ontology on ICT security issues will be composed next, a task that will entail three major activities: domain conceptualization of ICT security meaning a thorough understanding concerning entities and procedures in ICT security, actual development of the ontology on ICT security concepts to ensure complete coverage and usefulness, and context-based ontology integration to the Enterprise Mashup application. The latter means that enterprise specific use cases on the one hand, and ICT security policies on the other hand will guide the design of a bi-dimensional view of the Enterprise Mashup application. Finally, a database will be designed and developed to keep rules for ICT infrastructure security. The proposed system architecture is depicted in Figure 1.

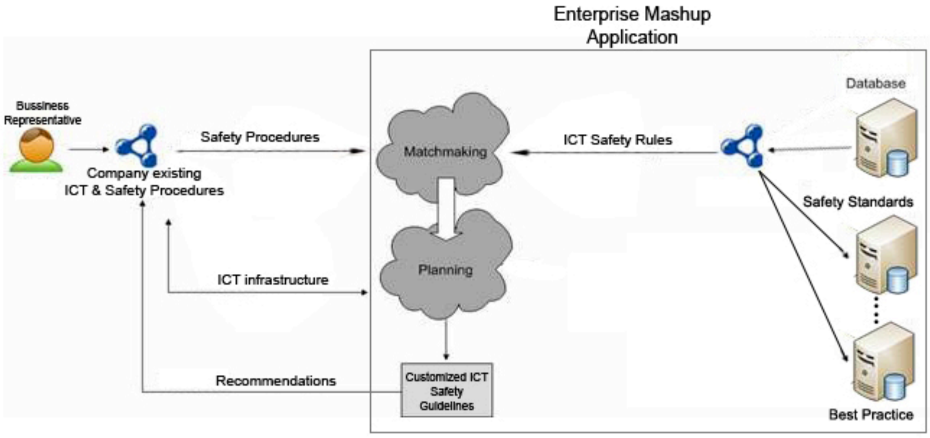

Figure 1. Mashup IT Security Application Architecture.

3 USER-DEPLOYED IT SECURITY PRACTICES AND STRATEGIES

A survey is being conducted among Cypriot organizations, both in public and private sectors, regarding established security policies and procedures on ICT security issues. Initially the target population was SMEs, however it was decided to expand the scope of the survey to include public organizations as well. A suitable and simple approach to identify these current security strategies deployed in organizations is to construct a comprehensive checklist where the respondent would simply indicate the presence or not of a security feature, technology, policy, or strategy. Thus, the survey questionnaire is heavily based on checklists that addressed all factors involving security policies and procedures, including ICT Security Management, ICT Security measures, Networking and Internet Connection. This section describes the format and content of the questionnaire and proceeds with presenting preliminary results.

3.1 Questionnaire Design Logistics

The Federal Office for Information Security (BSI) is a national security agency that promotes and provides IT security for the federal government in Germany. Its publication "*IT Security Guidelines*" (BSI, 2007) is a practical approach to security that provides a compact overview of the most important organisational, infrastructural and technical IT security safeguards, aimed at IT managers and administrators in small and medium-sized companies as well as in public agencies. These security guidelines were consulted during the process of designing the questionnaire on user IT security practices. Note that the local government does not provide such a document and we strongly believe that the BSI guidelines are comprehensive, yet simple enough for our purposes.

To be more specific, the questionnaire comprises of 11 sections, as shown in Table 1[1]. Sections *B* through *J* consisted of dichotomous questions that ask respondents to answer *yes* or *no* and are based on the security safeguard checklists outlined in the aforementioned document. The *Company Profile* section and section *A - Network Details* section also included open- and closed-format questions, so as to get demographical details for the organization and its network profile respectively. Companies with an IT department were requested to supply answers to all sections, whereas enterprises without a dedicated IT department only had to provide answers *to Company Profile* and *Network Details* sections.

Section	Questions	Topics
Company Profile	12	IT department structure (if any), business main activity, other company, demographical, and personal data
A – Network Details	11	Network topology and connectivity, security concerns, security technologies deployed (in-house, outsourced to third parties), current security practices, security incidents (embezzlement, fraud, theft of proprietary information, denial of service, vandalism or electronic sabotage, viruses)
B – IT Security Management	15	Objectives defined, human resources allocated, action plan documented and implemented, time intervals for security inspections, ongoing training of old and new personnel, etc.
C – Security of IT Systems	14	Protection mechanisms used, software installed, roles and profiles assigned to all users, privileges and permissions controlled, proper documentation created and updated regularly, etc.
D – Compliance with Security Requirements	6	Confidential information stored properly, confidential information handling in case of repair or maintenance of ICT equipment, security regulations monitored, security breaches properly reported and disciplined, etc.
E – Networking and Internet Connection	7	Firewall existence, configuration and functionality monitored, data visibility to outside users defined, unnecessary services disabled, etc.
F – Maintenance of IT Systems	3	Updates installed regularly, appointed personnel vigilant on required updates, test concept for software modifications, etc.
G – Passwords and Encryption	6	Types of password protection and encryption used, default passwords changed, secure passwords guidelines, safeguards on mobile ICT equipment, etc.
H – Contingency Planning	3	Contingency plan existence, adequacy of addressing all contingency situations, familiarity and accessibility of contingency plan, etc.
I – Data Backups	5	Strategy, implementation, regular control and updates, proper documentation, etc.
J – Infrastructure Security	5	Adequate protection against physical threats, sensitive areas physical protection, visitors protocol, intruders' protection, etc.

Table 1. Questionnaire Composition

[1] Note that due to space limitations, the actual 12-page questionnaire is not included in this paper. It is available on request.

3.2 Preliminary Analysis of Results

During the period starting April 1, 2010 and ending May 10, 2010 completed responses to the survey were received from 60 companies, in both the public and private sectors. There were 45 companies of company size less than 250 employees. It is expected to reach a sample size of approximately 120 companies by the end of the survey, which is estimated to be end of July 2010. The data was analyzed with the statistical package SPSS. The focus of the analysis, at this preliminary stage, was to determine the level of security awareness within organizations. With this in mind, Sections *B* through *J* constituted our survey's 9 attributes. Each question in these sections was assigned a score of 1 with a positive response, and a score of 0 with a negative response. A total of 33 companies had a dedicated IT department (55% of total contacts), with the remaining 27 being without an IT department (45% of total contacts).

Consider Figure 2 that illustrates the frequencies of each score for 4 attributes: *IT Security Management*, *Security of IT Systems*, *Compliance with Security Requirements*, and *Contingency Planning*. The *IT Security Management* chart indicates that there is no observation with score 0, the lowest being 0.13. Taking into consideration that 15 questions were grouped together for this attribute, the 0.13 corresponds to 2 positive answers (2/15). The highest frequency is observed at 1.00, which means that there are 15 out of 15 positive answers. A total of 6 companies answered positive to all questions.

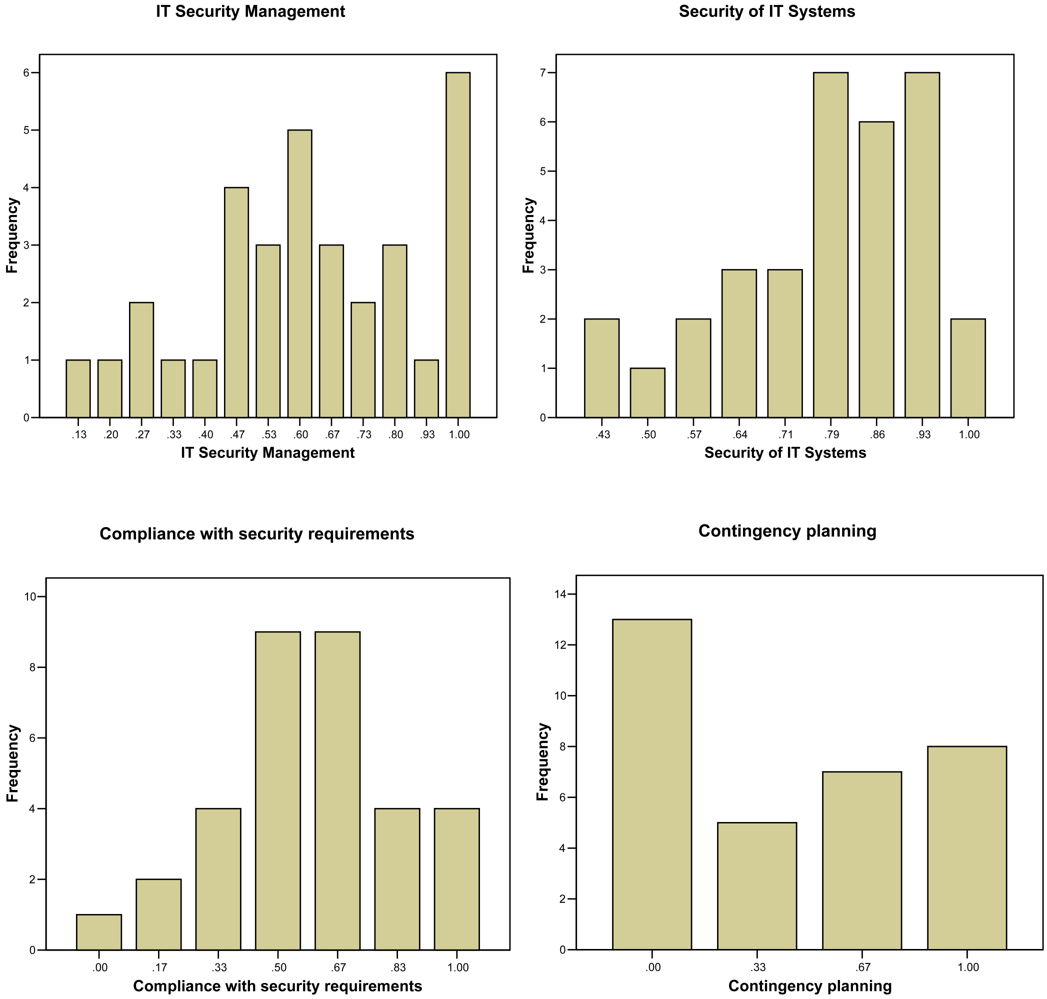

Figure 2. Score Frequencies for Selected Attributes

Most of the scores of *Security of IT Systems* attribute are between 0.79 and 0.93. There are two scores at 1.00. The lower score is 0.43, with two observations. The number of questions that are included in this attribute is 14; thus 0.43 corresponds to 6 positive answers. In the attribute *Compliance with Security Requirements*, there is 1 observation with 0 mean score and 4 observations with 1.00. The highest frequency is at .50 and 0.67 with both at 9 observations. Proceeding with the *Contingency Planning* attribute, 13 companies scored 0, whereas 5 scored 0.33, 7 scored 0.67, and finally 8 scored 1.00.

Table 2 shows the mean score of all attributes. The highest mean is observed in *Infrastructure Security* (0.8364). The group of high average includes *Security of IT Systems* (0.7792), *Data Backups* (0.7697), *Maintenance of IT Systems* (0.7677), *Passwords and Encryption* (0.7677) and *Networking and Internet Connection* (0.7662). The next attribute is *IT Security Management* with a score of 0.6323, followed by *Compliance and Security Requirements* (0.5909). The last place is given to the attribute *Contingency Planning* with a mean score of 0.4343.

Attribute	Valid	Mean
B – IT Security Management	33	.6323
C – Security of IT Systems	33	.7792
D – Compliance with Security Requirements	33	.5909
E – Networking and Internet Connection	33	.7662
F – Maintenance of IT Systems	33	.7677
G – Passwords and Encryption	33	.7677
H – Contingency Planning	33	.4343
I – Data Backups	33	.7697
J – Infrastructure Security	33	.8364

Table 2. Mean Score for All Attributes

The preliminary results of the questionnaire indicate that a majority of organizations in the sample have made provisions for security and its management. However, it is interesting to point out that only 28% of the respondents answered positively on the question "*Is there an IT Security officer?*" Even though this fact does not indicate a contradiction with the results obtained for the *IT Security Management* attribute that exhibits a mean of 0.6323, still investigation is needed to determine how security practices are carried out in these organizations.

4 CONCLUSIONS AND FUTURE DIRECTIONS

By addressing security aspects, organizations will be able to operate more efficiently: more specifically, the administration, planning and maintenance of ICT infrastructure will be managed in an efficient and effective way. Improved ICT security and workforce will have a positive feedback within the business organization leading to higher productivity as well as to offering improved services to customers and other business partners.

An ongoing research project initiated and currently pursued by researchers at University of Nicosia aims in developing a user-friendly Mashup security application that public and private companies could utilize and tailor according to their particular security needs and expectations. A survey that captures user practices in Cyprus was discussed in this paper, accompanied with preliminary results. The immediate short-term goal is to complete the survey and take an in-depth look at the results by analyzing the responses of all questions found in the questionnaire. A comprehensive case study on existing ICT security perceptions and practices among organizations in Cyprus will be thereafter composed. In addition, it would be beneficial to compare and contrast results with similar surveys contacted in other countries. This is something that will be also pursued in due course.

References

Bagchi, K., and Udo, G. (2003). An Analysis of the Growth of Computer and Internet Security Breaches, Communications of the AIS (12). pp. 684-700.

Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development, ACM Computing Surveys (25:4). pp. 375-414.

Federal Office for Information Security (BSI) (2007). IT Security Guidelines, Technical Report, available at https://www.bsi.bund.de/cae/servlet/contentblob/475854/publicationFile/28256/guidelines_pdf.pdf/, last accessed May 15, 2010.

Daniel, F., Matera, M., Yu, J. Benatalla, B. Saint-Paul, R., and Casati, F. (2007). Understanding UI Integration. A Survey of Problems, Technologies, and Opportunities. IEEE Internet Computing,11(3), 59-66.

Dhillon, G., and Backhouse, J. (2000). Information System Security Management in the New Millennium. Communications of the ACM (43:7), pp. 125-128.

Hoyer, V. and Stanoevska-Slabeva, K. (2009). Generic Business Model Types for Enterprise Mashup Intermediaries, Proceedings of the 15th American Conference on Information Systems (AMCIS)

Hoyer, V. and Staneovska-Slabeva, K. (2008). The Changing Role of IT Departments in Enterprise Mashup Environments. Proceedings of the 2nd International on Web APIs and Service Mashups.

Hoyer, V., Stanoevska-Slabeva, K., Janner, T., and Schroth, C. (2008). Enterprise Mashups: Design Principles towards the Long Tail of User Needs. In IEEE International Conference on Service Computing (SCC'08). Volume 2, 601-602.

Liang H. and Xue Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly. 33(1), 71-90.

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly (16:2). pp. 173-186.

Maximilien, E.M., Ranabhu, A., Godmadam, K. (2008). An Online Platform for Web APIs and Service Mashups. IEEE Internet Computing, 12(5), 32-43.

Stafford, T. F., and Urbaczewski, A. (2004). Spyware: The Ghost in the Machine," Communications of the AIS (14), pp. 291-306.

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

Yu, J., Benatallah, B., Casati, F., Daniel, F. (2008). Understanding Mashup Development. IEEE Internet Computing, 12(5), 44-52.