INFORMATION SECURITY AWARNESS IN DIFFERENT HIGHER EDUCATION CONTEXTS
A Comparative Study

Adam Marks[1] and Yacine Rezgui[2]
[1]*Department of Business Administration, World-Wide, Embry-Riddle Aeronautical University, Daytona Beach, FL, U.S.A.*

[2]*School of Engineering, Cardiff University, Queens Buildings, The Parade, Cardiff CF24 3AA, Wales, U.K.*

Keywords: Information Security, Awareness, Higher Education, Human Factors.

Abstract: Higher education in the UAE has advanced significantly in the last decade. Several higher education institutions have been seeking/granted international recognition and accreditation. Yet, the status of IT in UAE higher education has received very limited attention. This study explores and compares the level of IS security awareness of IS users in one of the leading UAE higher education institutions to those of IS users in a classical UK university. In addition, the study looks for possible factors behind any possible variations on the levels of IS security awareness.

1 INTRODUCTION

The quantity of scholarly work regarding the intersection of information technology and higher education in developed countries has been relatively limited. This limited attention is even more apparent in the case of developing countries where other factors such as lack of resources and infrastructure, lack of knowledge, and sometime language and other sociological barriers may come into play. The role and status of IT in the Middle East, with the exception of a few countries, have been largely ignored until the mid 1990s (Goodman, 1991).

In the past decade, the UAE has launched a series of IT education initiatives designed to sharply raise the technology skills of the UAE population (Martin, 2005). In 1998, Zayed University was established as the first UAE-national University with an international curriculum, and with English as the language of instruction. In addition, in the recent few years, a number of US and other foreign universities have opened branch campuses in the UAE, including Middlesex University from the UK, University of Wollongong from Australia, and University of Michigan from the US (Mani, 2006). As a result of this global networking and the extending reach of universities beyond their traditional boundaries, Information Systems (IS) security is emerging as a significant concern.

Information Technology (IT) in higher education can be characterized by equipment diversity, IT decentralization, and user diversity (EDUCUASE, 2003). Experts in computer security agree that universities are among the least Information Systems secured environments. Only a third of the examined universities had security awareness training for students and faculty (North, 2006). Colleges and universities are targeted for cyber attacks for two main reasons. First, is the vast amount of computing power they posses; and second, is the open access they provide to their constituents (EDUCAUSE, 2003). Universities also have a considerable amount of confidential information that makes them prone to IS security threats (Katz, 2005).

While most managers pay more attention to technical tools such as firewalls, and intrusion detection software; they seem to focus less on soft issues such as the hazards caused by end users' lack of awareness (Katz, 2005). Managers and employees tend to think of IS security as a second priority compared to their own efficiency or effectiveness issues, because the latter have a direct impact on the outcome of their work (ISACA, 2006). In addition to all the above, while information security awareness is commonly recognized, the number of studies that

Marks A. and Rezgui Y. (2010).
INFORMATION SECURITY AWARNESS IN DIFFERENT HIGHER EDUCATION CONTEXTS - A Comparative Study.
In *Proceedings of the 12th International Conference on Enterprise Information Systems - Human-Computer Interaction*, pages 215-222
DOI: 10.5220/0002888102150222

consider it in depth is limited. This is may be attributed to (a) the non-technical nature of security awareness (Siponen, 2000), and / or (b) its scope, as it falls outside the traditional engineering and hard computer science domains (Dunlop, 1992). Organizations with strong technical security countermeasures may still fail to protect their information systems. The human factor is considered the weakest link in the IS security chain (Mitnick, 2002).

The purpose of this study is to explore the levels of information systems security awareness of IS users in one of the premiere universities of a developing country, namely Zayed University in the UAE, in compare to those of a traditional university of a developed country, namely the University of Salford in the UK. The study also seeks to explore the key factors behind any possible variation in the IS security awareness levels of the examined environments. To conduct the research, an interpretive case-study approach was employed using multiple data gathering instruments. This paper contains 8 sections. Following this introduction is the methodology of the research, literature on Information Security Awareness, the status of IS in the UAE and Zayed University, the findings of the study, discussion of the findings, conclusion, and then the references.

2 METHODOLOGY

Within the context of international higher education in general, and the context of Zayed University (and, both directly and indirectly, institutions of higher education within the UAE), the proposed research aims to explore and compare, on the one hand, the level of IS security awareness of IT users (Faculty and Staff) at higher education institutions in the UAE, to that of IS users (Faculty and staff) at higher education institutions in the UK. On the other hand, the research seeks to explore the key factors behind possible variations, if any. The paper addresses the following main research question:

• How do the levels of IS Security awareness of IS users in UAE higher education compare to those of the UK higher education?

• If variation exist between the compared two IS security awareness levels, what are the key factors behind the variation?

While most if not all information systems security awareness studies have been conducted in developed countries, and within a western context; no significant study has been reported in the case of developing countries, especially the UAE. In addition, while most existing studies seem to focus on the technical elements of information systems security, they seem to overlook in their majority the socio-cultural and organizational aspects of IS security. The proposed research contributes to the body of knowledge by addressing the identified gaps. An interpretive case-study approach is employed to conduct the research. Two case studies have been selected: a major case study in Zayed University in the UAE where one of the researchers previously held employment, and a minor case study in the University of Salford in the UK where the same researcher conducted his doctoral studies. The access the researchers had to both universities in terms of information, documents, personnel, other university resources, and ability to observe for extended periods of time was another key reason for this research as well. The countries chosen for the study are both established in terms of IT infrastructure and thus provide a comparable base that is relatively free from the noises of other unrelated factors. In addition, the fact that the authors have access to the research subjects in both countries and have a fairly good understanding of the two cultures and languages also made such comparative research feasible.

Zayed University was established in 1998 by the federal government of the UAE to educate UAE National women with no tuition fees. The university focuses on education and learning, while paying less focus to research. The university relies largely on government funding. The number of enrolled students in 2006 was approximately 3000 students. The university is based on an international model of higher education with the primary instruction language being English. The great majority of the 700 staff members come from the USA, Europe, and Australia. Zayed University is IT orientated and it offers several online services to students and staff. The university is well regarded within the UAE. (Zayed University Web Site, 2006). The University of Salford is an enterprising university based on Manchester, UK. The university history goes back to 1896. Today, the University of Salford educates more than 18000 students with the help of more than 2500 staff members. The university is research orientated in many fields, including virtual reality, magnetics and optics, genetic algorithms, building design and prosthetics. Over 3,000 international students from 80 different countries are enrolled in the University's 14 schools and 13 research institutes. The university does not rely only on state

funding, but also other sources of income including tuition fees. The great majority of staff is home grown (University of Salford Web Site, 2006).

In this research study, both qualitative and quantitative research paradigms were chosen. An interpretivist stance is chosen to provide focus and structure throughout all phases of research and data collection (Denzin, et al., 2000; Myers, 1997; Orlikowski, et al., 1991). An Interpretivist approach is more appropriate since the researcher is not independent of the study.

To ensure consistency and validity of findings, multiple sources of data were gathered through the use of four main instruments: Interview, Questionnaire, Documentation, and Observation. As stressed by (Bonoma 1985), collecting different types of data by different methods from different sources produces a wider scope of coverage and results in a fuller picture of the phenomena under study than would have been achieved otherwise. The development of converging lines of inquiry in this manner is known as "triangulation", and is generally considered as a process of using multiple perceptions to clarify meaning and verifying the validity of an interpretation (Stake, 1995). Pattern coding (Miles, 1994) was also used to identify emergent themes, patterns, or explanation suggested by qualitative information gathered from the selected instruments. To measure the levels of users IS security awareness; the sources of data of this study targeted the following 10 themes:

- User's IS security awareness of available and accessible IS systems.
- User's IS security awareness of existing IS security policies, standards, and guidelines.
- User's IS security awareness of existing IS security laws and legislation.
- User's IS security awareness of available IS staff and personnel.
- User's IS security awareness of possible IS security threats and concerns.
- User's IS security awareness of possible IS security solutions.
- User's IS security awareness of available IS security training session and materials.
- User's IS security awareness of available IS security documents and help material.
- User's IS security awareness and perception of the value of university data.
- User's IS security awareness and perception of his/her role in university's IS security.

The UK (Salford) case study relied on a large number of semi-structured extensive interviews (10) conducted with managers and directors from the Information Services Division (ISD); the results of 89 questionnaires, documentations, and observation of the researcher(s); while the UAE relied on 12 extensive interviews with IS policy and decision makers, 143 questionnaires, documentations, and observation of the researcher(s).

It is important that the limits of this study be recognized as the researcher relied on information that was publicly available or given through questionnaire and interviews. It is always possible that pertinent information might have been held for commercial, strategic, or political reasons. In addition, access to national documents in the UAE was not always successful. Another potential limitation of the study is that it relied mainly on the findings of two case studies in the UAE and in the UK. Although it can be argued that these institutions are typical of universities in the selected countries, the research would benefit from further case study universities from these countries as well as other developed and developing countries.

3 UNITED ARAB EMIRATES (UAE) – ZAYED UNIVERSITY

Developing countries differ from developed ones not only because they have less capital but also because they have less knowledge (Abdullah, 2004). However, over the last decade, the UAE has shifted itself to become the hub for telecommunications and information technology in the Middle East. The government of the UAE has funded significant projects in e-commerce and information technology related industries such as Dubai Internet City, and Dubai Silicon Oasis (Kostopouls, 2003). The rapid growth in IT is evident from their improvement in the position of e-governance ranking, e-readiness ranking, and networked readiness index ranking. A recently released UNDESA report placed the UAE at number 42 in the world in terms of e-government readiness, but number one in the Gulf region. The report also indicated that the UAE had moved up 18 places from 2004, when it was ranked 60th in the world. However, while the importance of IT is not disputed in the Middle East, the main problem lies in the way IT is managed and applied, Booz, Allen, and Hamilton study titled "Information Technology in the Middle East" suggests. The study attributes the ineffective application of information technology in the region to the general absence of strategic IT planning; the lack of available-skilled staff; and the

general absence of IT-performance measurement system (Barrage et al, 2003). In terms of IS security, the region has a large underground market for illegal software (Joseph, 2006). According to Kevin Isaac, regional director, Symantec Middle East, and Africa, the Middle East leads the world as the source of Internet threats per capita. Isaac attributed the increased number of attacks in the region to the increased number of networks, the adoption of ADSL, and abandoning monopolistic practices in the telecommunications sector, bringing cheaper and faster Internet connectivity. The increased connectivity is accompanied by an increased number of unaware users who can easily become easy targets to criminals and hackers. The UAE ranks first among the countries monitored in the region, both in terms of origination of attacks and targeting by online fraudsters. The UAE is ranked 46 globally as an originator of phishing attacks. The UAE's high economic profile, combined with the availability of the latest technologies, makes the country more prone to online attacks than other GCC countries. Measures such as forming a Computer Emergency Response Team (CERT), and the passing of IT legislation, are being considered to curb the attacks (Emirates Today, 2007; Khaleej Times, 2007).

Zayed University's IS infrastructure is highly comparable to institutions in UK and the US. Each student purchases a laptop upon entry to the university and each faculty member receives a laptop with a three-year replacement schedule. Electronic communication is the standard mechanism of communication for faculty and students. Each classroom has a network connection for each and every seat. The classroom also has a projector, printer, and a spare workstation. Email and Internet is easily accessible. Blackboard is used as a course management system to build an electronic interaction between the faculty and student (Zayed University Self Assessment, 2004; Zayed University Self Study, 2006).

4 INFORMATION SECURITY AWARENESS

Information security may be defined as the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use (McDaniel, 1994). While information security in general is focused on the confidentiality, integrity, and availability of information; information security awareness is concerned with creating and maintaining security-positive behavior (Kruger, 2006). According to the Information Security Forum (ISF, 2003), information security awareness can be defined as (a) the degree to which every user understands the importance of information security, (b) the appropriate level of information security to the organization, (c) users' security responsibility, and (d) users' behaviors and acts. Siponen (2000) defines information security awareness as the state where users in an organization are aware of, and ideally committed their security mission defined by the organization's end-user security guidelines.

The majority of today's IS attacks are not concerned with only circumventing the authentication process of an individual or an organization; they are more inclined to access confidential information. This has resulted in IS threats like phishing, identity theft, and social engineering (Dlimini, 2008). Yet information security continues to be ignored by many top managers and employees alike. IT executives have frequently identified the security of information as an important but not critical issue. The result of this neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary" (Straub, 1998). IS security awareness is often overlooked (Rezgui, 2008). Researchers believe that the effective implementation and use of IS security awareness practices can lead to improved security for organizations. Bray, (2002) suggests that in order to avoid IS security breaches, organizations should provide users with IS security awareness training programs. The training program should cover areas like social engineering, password protection, and heightened physical security alertness. Kovacich (2003) takes a step further by suggesting that organizations should implement a continuous security awareness training programs as part of the corporate asset protection program. While information security is a key organizational goal and users have a responsibility to maintain this goal, it is important however to understand that the implementation of an information security awareness program does not warrant that all users within the organization will understand their roles and responsibilities when it comes to information security (Albrechtsen, 2009). Perhaps, this is why Puhakainen (2006) recommend a combination of measures to increase users IS security awareness.

Puhakainen suggests that organizations use IS security awareness training, campaigning, and reward and punishment to establish an effective IS security awareness program. Cooper (2008) believes that Continuous reinforcement of proper IS security practices is needed to remind individuals of their role in information security. Both Rezgui (2008) and Kurger (2006) recommend that a systematic approach to measure the effect of a security awareness program should be implemented to evaluate the contribution and the return on investment of such programs (Kruger, 2006).

5 FINDINGS

5.1 User's IS Security Awareness of Available and Accessible IS Systems

The data evidence gathered indicate that the majority of users in both universities were aware of available IS resources. Examined IS users referred to the availability of email, Internet, Intranet, extranet, IP telephony, wireless connectivity, course delivery, and administration applications, e-library system, and electronic databases. In addition to identifying what IS services were available, most respondents were also able to explain the intended use of these services.

5.2 User's IS Security Awareness of Existing IS Security Policies, Standards, and Guidelines

The two examined institutions varied considerably under this category. Zayed University did not have any IS security policies, standards, or procedures in place, while the University of Salford did. In terms of awareness, 84% of the examined IS users in Zayed University could not confirm the existence of existing IS security policies, standards, and guidelines. 76% of the examined IS users in Salford confirmed the existence IS security policies, standard, and procedures.

5.3 User's IS Security Awareness of Existing IS Security Laws and Legislation

All examined IS users in Zayed University were not aware of the 2006 IS legislation in the UAE. 68% of the examined IS users in Salford referred to the Computer Misuse Act and the Data Protection Act. 90% of these users were informed through the Information Services Division, while the remaining 10% were informed through other resources.

5.4 User's IS Security Awareness of Available IS Staff and Personnel

32% of examined IS users in Zayed University were able to identify whom and how to reach for an IT-related issue. 76% of the examined IS users in Salford referred to the availability of the names, roles, and contact information of all ISD employees in ISD web page. The web page displays the organizational structure of ISD. The Information Services Division in Zayed University maintained a web page for the university, but did not maintain a web page for the division.

5.5 User's IS Security Awareness of Possible IS Security Threats and Concerns

74% of IS users in Salford were able to identify several possible IS security threats including denial of service, social engineering, shoulder surfing, and email spam, compared to 18% in Zayed University.

5.6 User's IS Security Awareness of Possible IS Security Solutions

IS users in Salford also scored higher than their counterparts in Zayed in terms of awareness of IS security solutions. 82% of IS users in Salford were familiar with security solutions including data back up procedures, virus protection, and password protection rules, compared to 16% of the examined IS users in Zayed University.

5.7 User's IS Security Awareness of Available IS Security Training Session and Materials

Although the Information Services Division offers periodical training session in Microsoft Office applications, it did not offer a single IS security training since the university inception in 1998. Naturally, none of the examined users were aware of any IS security training sessions. IS users ate the university of Salford are required to attend an IS security training session as part of their orientation (Faculty, staff, and students). In addition to the

mandatory session, the IS security coordinator offers periodical sessions throughout the academic year.

5.8 User's IS Security Awareness of Available IS Security Documents and Help Material

Similar to the training category, IS users in Zayed University were not aware of IS security documents and help material. Zayed's Information Service Division did not have any in place. 34% of IS users in Salford were able to reference IS security document and help materials.

5.9 User's IS Security Awareness and Perception of the Value of University Data

46% of the examined IS users in Zayed University viewed university data as private and confidential, while 54% viewed the university data as "of no interest to anybody". Inversely, 96% of the examined IS user in the University of Salford viewed university data as private, confidential.

5.10 User's IS Security Awareness and Perception of his/her Role in University's IS Security

In this last category, 88% of the examined IS users in Zayed University believed that they have a very limited role in IS security, and that the full responsibility falls on the shoulder of the Information Service Division. 98% of the examined IS users in the university of Salford believed that they have a shared role in protecting the information of the university.

6 DISCUSSION AND RECOMMENDATIONS

The first research question of this study compares the level of IS security awareness of IS users in UAE to that of the UK. The findings of this study indicate a considerable difference in the level of IS security awareness of IS users in the two examined higher education institutions. IS users in the University of Salford were more aware of IS security-related matters than their counter parts in Zayed University. Unlike IS users in the University of Salford, most IS users in Zayed University were not aware of possible IS security threats and how to defend against them; they were not aware of whom to reach in case of IS security problem; they were not aware of the proper policies, standards, and guidelines that should govern their access and use of IS systems; and, most importantly, they were not aware of their own role in defending against IS security threats and protecting university data. The second question of this study seeks to understand the factors behind this varying level of IS security awareness. While the IS infrastructure in terms of software, hardware, communication, and people resources in the examined two universities was comparable, and while the two examined higher education institutions employed similar IS technical solutions, what varied mostly was the level of IS security awareness tools and activities utilized by each institution. The IS security function in The University of Salford appeared more supported, coordinated, regulated, and centralized than in Zayed University. IS users in Zayed University reflected a low-perceived value of the importance of IS security and the data stored by the university. This low-perceived value is a natural result of the lack of emphasis shown by the university management, which is represented by the following:

- The lack of IS security training.
- The lack of IS security policies.
- The lack of IS security coordination.

Inversely, the higher level of IS security awareness in Salford can be attributed the university commitment to IS security awareness, represented by:

- The establishment, communication, and enforcement of IS security policies.
- The establishment, communication, and enforcement of IS security training programs.
- The establishment and enforcement of of IS security coordination.

Only through the establishment, communication, and enforcement of theses activities that IS users can be properly be informed of the organization's stance and their individual roles in terms of IS security (Rezguie, 2008). Because many aspects of information security involve technology, it is so easy for IS users to think that the problem is being handled by the IT department and other technical solution (Mitnick, 2002). These IS users may inadvertently and easily cause harm to the university and its IS systems if they users fall victim to a simple social engineering attack, or if they open a malicious email. This lack of emphasis on IS security awareness in Zayed university could be linked to a larger lack of emphasis by the federal

government. Which is seen in the quantity and quality of legislation that addresses IS security and data protection in the UAE versus other countries such as the UK or versus other types of legislation. The UAE has only one law that was issued in 2006 to address cyber crimes. This law is young, immature, and yet to be challenged. The UAE court system has not witnesses a single case where one of the government institutions was accused of liability for data exposure.

It is the conclusion of the authors, and in correlation with the findings of (Mitnick, 2002), and (Puhakainen, 2006), that the following steps have the potential to increase the level of IS security awareness, and consequently the level of IS security in UAE higher education: (a) Establishment of IS security policies and procedures; (b) Campaign IS security awareness best practices and advertise IS security training sessions and materials; (c) Train users on IS security best practices to increase their awareness; (d) Practice reward and punishment.; and (e) Conduct continuous evaluation and readjustment.

7 CONCLUSIONS

This paper explores the level of IS security awareness of IS users in UAE higher education and compares it to that of IS users in UK higher education. The findings of this study indicate that despite the fact that the IS infrastructure of the examined institutions is relatively comparable, the level of IS security awareness of IS users in the UAE was considerably lower than that of IS users in the UK. This gap of IS security awareness can directly be linked to the level of organization commitment to IS security awareness activities in the case of the UK, and the lack thereof in the case of the UAE. The organization's commitment to IS security awareness in the case of the UK could be represented by the establishment, communication, and enforcement of IS security awareness measures such as IS security policies, IS security training, IS security documentations, and IS security coordination. While none of these measures were found in the case of the UAE. This organization's level of commitment to IS security awareness is also a indication of the organization's perceived value of the data it stores. While some of these findings may sound basic in nature. In retrospect, they appear to be something that you would fundamentally expect to be addressed in any higher education institution that aspires for international accreditation and recognition.

REFERENCES

Abdullah, A., 2004. The Development of Electronic Journals in the United Arab Emirates University (UAEU).

Barrage, G., Majdalani, F., Vayanos, P., and Shehadi, R.,2003. Information Technology in the Middle East: The CEO Agenda. *Booz, Allen, and Hamilton*.

Bonoma TV., 1985. Case Research in Marketing: Opportunities, Problems, and a Process. *Journal of Marketing research.* 22:199-208.

Bray TJ., 2002. Security actions during reduction in workforce efforts: what to do when downsizing. *Information system security*. 11-15.

Cooper, M., 2009. Information Security Training- Lessons Learned Along the Trail. *Proceedings of the 36th annual ACM SIGUCCS conference on User services conference*. 207-212.

Dlimini, M. T., Eloff, J. H. P., and Eloff, M. M., 2008. Information security: The moving target. *Computers & Security.*

Denzin, N. K., & Lincoln, Y. S. (Eds.), 2000. The handbook of qualitative research. (2nd ed.). London: *SAGE Publishing*.

Dunlop, C. &Kling, R. Social Relationship in Electronic Commerce., 1992. Introduction in Computerization and Controversy- Value Conflicts and Social change, (ed. C. Dunlop and R. Kling). *Academic Press*, New York, USA.

EDUCAUSE center for Applied Research: Information Technology Security: 2003. Governance, strategy, and practice in Higher Education.

Emirates Today. UAE Rank 46th Globally as Originator on Phishing Attacks. Retrieved 22, March, 2007 from http://www.ameinfo.com/56212.html.

Goodman, S.E., 1991. Computing in a less developed country. *Communications of the ACM*, 34, 12, 25-29.

ISACA. Information Systems Audit and Control Association., 2006. Information Systems Auditing Manual.

ISF- International Security Forum., 2005. The Forum's Standard of Good Practice for IS security. Cited May 18th 2006 from http://www.isfsecuritystandard.com/index_ie.htm.

Joseph, M., 2006. IT in the Middle East: Overview. *Proceedings of the 7th conference on Information technology education*.

Katz, FH., 2005. The Effect of a University Information Security Survey on Instructing Methods in Information Security. In: *Proceedings of the 2nd annual conference on Information security curriculum development.* p.43-48.

Kostopoulos, G., 2003. E-Government of the Arabian Gulf: A vision Toward Reality. *ACM International Conference Proceeding Series;* Vol. 130.

Kovacich GL., 1998. Information system security Officer's Guide: Establishing and Managing an Information Protection Program. USA: *Butterworth-Heinemann*.

Kruger, H. A. and Kearney, W. D., 2006 A prototype for assessing information security awareness. *Computers & Security,* 25:1, pp. 289-296.

Mani, J.P. and Barry M. Lunt., 2006. IT in the Middle East: An Overview.

Martin, C.D., 2005. Removing the Veil. Personal Reflection on Educating Women in the Dubai.

McDaniel, G., ed., 1994. IBM Dictionary of Computing. New York, NY: McGraw-Hill, Inc.

Miles MB. and Huberman AM., 1994. Qualitative Data Analysis, An Expanded Source Book. Beverly Hills: Sage.

Mitnick, K. D., & Simon, W. L., 2002. The Art of Deception: Controlling the Human Element of Security, Indianapolis, IN: Wiley.

Myers, M. D., 1997. Qualitative Research in Information Systems. *MIS Quarterly*, 21(1), 241 - 242.

North Max M, Roy George, North Sarah M., 2006. Computer Security Ethics Awareness in University Environments: A Challenge for Management of Information Systems.

Orlikowski, W.J., 1993. CASE tools as organizational change: Investigating incremental and radical changes in system development. *MIS Quarterly*, 17(3), 309-340.

Puhakainen, P., 2006. A Design Theory for Information Security Awareness.

Rezgui Y, Marks A., 2008. Information Security Awareness in Higher Education: An Exploratory Study, *Computers & Security*.

Siponen, M.T., 2000. A Conceptual Foundation for Organizational Information Security awareness. *Information Management & Computer Security*, Volume 8, Issue 1.

Stake, R.E., 1995. The Art of Case Study Research, *Thousand Oaks:* Sage, 1995.

Straub, D.W. and Welke, R.J., 1998. Coping with systems risk: Security planning models for management decision making. MIS Q. 22, 4, 441–469.

University of Salford Web site – home page. Retrieved 02, February, 2006 from www.Salford.ac.uk.

Zayed University., 2006. Self Study Design Prepared for Middle States Commission on Higher Education.

Zayed University., 2004. Self-Assessment Document Prepared for Middle States Commission on Higher Education.

Zayed University Web site – home page. Retrieved 20, June, 2006 from www.zu.ac.ae.