Securing Security through Education

Karen Neville
University College Cork, Ireland
Kneville@afis.ucc.ie

Philip Powell
University of Bath, United Kingdom
mnspp@management.bath.ac.uk

Abstract

Traditionally security has been the pervasive factor in organizational growth but its importance has surpassed that of any other issue in retaining a competitive advantage. Security is, therefore, of paramount importance in the retention of organizational innovation. The key in building a secure environment lies in an organizations ability to react to changing threats both from within and external to the case. The objective of security is to protect corporate knowledge as well that of the tangible asset. It is ironic that to secure knowledge the organization must expand its knowledge of security. To this end universities are currently striving to produce educational programmes to meet industrial demand for this core requirement. The amalgamation of theoretical research and industrial practice in Third level programmes is vital to ensure ongoing industrial support for academia. To this end the case under investigation strives to produce IT graduates with the ability to utilize theoretical knowledge, particularly of security, in a practitioners domain. The construction and implementation of any course is very much emergent, given the unique institutional nature of academic programmes. This paper conducts an analysis of an approach in delivering practical, as well as theoretical, knowledge of security, using a unique project to enable the learners to utilize the theoretical knowledge gained through the classroom.

Keywords: Security, Knowledge, Education

Introduction

This paper focuses on the design of a suitable course to support learners and encourage co-opetition. The research outlines the factors necessary for the successful understanding of the complexity of the relationship between security and knowledge (the asset that is trying to protect), through the investigation of current research and the analysis of the case environment undertaken by the learners. It also highlights the potential of the programme to overcome the limitations of the traditional classroom due to increased student number. Group projects can, when properly mediated and structured, facilitate co-operation (Entwistle, 1997), reduce conflict and avail of all of the benefits that technology can provide (Johnson and Johnson, 1990) as well as the obvious advantages of controlled class competition.

Theoretical Foundation

Education should, to be effective, follow a model that can stimulate the mind (Kyllonen and Shute, 1989; McCormack et al, 1997). Psychology, as well as being the study of the human mind, is also that of human behavior. Psychologists have pursued this belief in the behavioral implications for education. However, you do not have to be a psychologist to create an effective learning environment but an understanding of how people learn helps (Ward, 1926). Another component intertwined in the learning methodology is group collaboration (Wells, 1992) and competition. The collaborative

or group model assigns specific roles in learning, and each participant communicates through this network (Luetkehans et al., 1996; Driscoll, 1998) of groups. Groups are defined as people who are aware of one another and have the opportunity to communicate (McGrath, 1984). The study of people as individuals and in groups started as early as the 19th century. For example, Gustave Lebon (1896) investigated the absorption of individuals into a crowd, loosing their personality and adopting the collective mind of the group, be it a departmental group (Huczynski and Buchanan, 1985) or a group of students. The behavior of individuals will change in the presence of other individuals (Argyle, 1994; Adam, 1999), it has long since been established that individuals can be expected to perform better or worse when they are observed or supported by others (Baron and Byrne, 1977). The role that groups come to play in their organization or university cannot easily be tied down to simple models (Adam, 1992). The word group seems to suggest co-operation and collaboration in any environment, be it organizational or educational. However, research is full of as many examples of conflicts as co-operation (Putnam and Poole, 1987; Easterbrook, 1991). Group work when properly structured and mediated enables productive collaboration and intra-group competition. Increases in student numbers necessitates structuring in the traditional classroom. Structured communication provides both the educator and learner with the following advantages: (1) access to expertise without conforming to the opinion of the class; (2) anonymity of the participants through the group; (3) opportunity to participate in a large group and (4) a mediator (instructor) to assure the flow and value of the discussion. If these are incorporated into any learning network the approach will succeed in supporting the learner. The roles of educators and students are changing (Jonassen et al, 1996; Driscoll, 1998). This method of group work or group projects is more individualized when compared to the traditional classroom as peer interaction and collaboration are also emphasized resulting in a learning paradox when the individual learner can excel in groups. This learning approach is designed to provide greater support to the learner to allow everyone the opportunity to speak without conforming to the pressures of the larger classroom but also benefiting from controlled co-opetition. An educational model should, to foster effective learning, provide the learner with both explicit and tacit knowledge, be the subject security or programming.

Knowledge

Buckingham et al., (1987) define information as...*explicit knowledge'*, the significance of which is that information has meaning and it is clearly understood. Knowledge is regarded as volumes of relevant information but, importantly, in addition to experience (tacit knowledge) in the form of an expert (Avison and Fitgerald, 1997). Therefore knowledge cannot be easily defined or explained, resulting in numerous research papers and philosophers who debate it's meaning. It is a combination of a number of factors that are interpreted by the expert or knowledgeable person making the decision. Knowledge is regarded, in this information driven economy (Drucker, 1993) as *power* or a source of competitive advantage (Laudon, 2000; Grant 1996; Drucker 1993). However organizations face the dilemma of protecting this knowledgebase from both internal and external risks. Relationships form when groups within an organization cooperate to achieve a common goal and external relationships are formed (as in the classroom) to provide a mutually beneficial service. Information is gathered through these communication networks composed of individuals, groups, departments and organizations cooperating and competing to possess useful knowledge. Organizations must therefore manage the risk via such an open network. In today's virtual communication networks, knowledge transfer has extended from passing information from individual to individual (Cantoni et al, 2001) to moving knowledge from one point in the organization (or virtual organization) to another (Rutkowski, 1999). However problems pertaining to knowledge creation arise due to lack of ongoing training/education, employees leaving, and a lack of internal collaboration resulting in duplication of work or internal competition. While knowledge may be a key organizational resource, it will only provide sustainable competitive advantage if it is protected. Understanding of security has expanded to include collaborating with competitors and virtual relationships, resulting in complex interactions and risks. Individuals form ties with peers and others to collaborate and create

knowledge. Knowledge creation depends on sharing and protection, but these interact, as a secure environment is necessary to create knowledge but knowledge of security is necessary in the provision of a secure environment.

Security

A security strategy is needed to protect valuable knowledge and data resources (Castano *et al.*,1994). Security goes hand in hand with dependency and any organization that adopts widespread implementation of information systems and trust relationships with third parties must accept that it is exposed to both accidental and malicious damage. An effective security model is a key strategic issue. In particular, the initiative for implementing a programme of risk management must be taken at the strategic management level and should be treated as an important corporate standard (Greenstein et al, 2000; Whiteley, 2000). Only when it is given this status will it be properly implemented. The main tasks involved in developing a security model to protect the corporate knowledge base are divided into two phases. First avoiding or reducing the risks in the first instance through both internal and external countermeasures (the provision of an effective security strategy and culture), then planning to cope with all eventualities if the worst should happen, through the provision of a contingency plan (Gollman, 1999) in place. Security can both hinder and enable the collection of data, the process of information retrieval and therefore the expected creation of knowledge. The complexity of both knowledge and security is undeniable. However, it can be argued that the two areas are intertwined. Both security and knowledge are among the primary goals of any organization, the levels of both are often exaggerated and balanced to produce a compromised output. Therefore security is a vital component in the ongoing creativity of a competitive environment (see Figure 1). The reliance of knowledge management and creation on existing and future interrelationships is evident yet difficult to validate. An organization is viewed as a col-

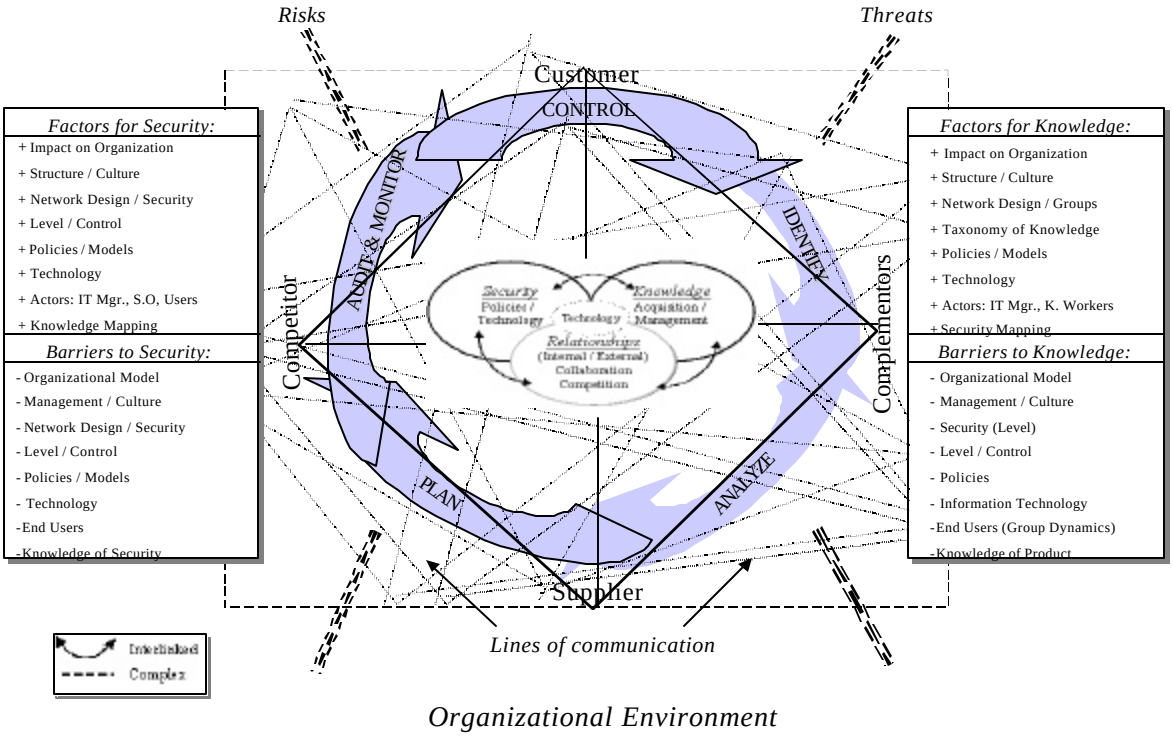

Figure 1: The Security & Knowledge Framework

lection of relationships and knowledge gained as a result (Tiwana, 2001; Wenerfelt, 1984). Large organizations with the ability to protect valuable knowledge have incentives to be innovative (Powell et al, 2001) and therefore remain competitive even through co-opetition. It is the technology that binds both security and knowledge together. Organizations use technology to both collect and share knowledge, while simultaneously protecting it.

Technology

Technology is used to collect and store data (Whiten et al, 1994) in order to produce valuable information (Connelly and Begg, 2002). Technological changes, in both secure hardware and software, are as constant as the increase in threats to corporate security (Greenstein et al, 1998). Secure protocols, standards and encryption are used to protect communication networks (Stallings, 2001) and devices such as firewalls and secure routers are used to filter out possible threats (Panko, 2000). However, designing network security and defining access control lists to control internal users is useless if the structure of the organization is devoid of the actors necessary to promote a culture of security awareness and knowledge of the approaches necessary to limit the threats posed (Goldman, 1998).

Therefore the incorporation of security and knowledge into a third level educational model is a true amalgamation of theoretical research and effective secure industrial practice. The study of both the interdependent relationship between security and knowledge and the factors required for the successful understanding of both is a valuable exercise in producing graduates with an understanding of the complexity of the inter-relationship and effectively producing the necessary security-knowledge workers.

Research Objective

This research study outlines the development and implementation of an educational model to meet the educational requirements of industry. The authors propose to expand the learners understanding of security through the incorporation of both explicit and tacit knowledge and through the utilization of problem-solving approaches to learning. Students will also avail of group collaboration and intra-group competition to produce the most effective security strategy for a fictitious bank and then present to a panel of industrial as well as academic experts, their security design, which must meet any security threat, identified by the panel. It is also the objective of this paper to examine the factors necessary for both the successful implementation of both security and knowledge and therefore learning. This will be achieved through the removal of the physical barriers imposed by the traditional classroom allowing the students to assume the roles of security officers, network administrators and hackers to accomplish the task at hand. Finally the authors propose to prove, in further research, that security and knowledge are interlinked within an organization, when security is either too high or too low knowledge creation is dramatically affected and a necessary balance is needed to create a knowledge and security oriented culture. It is therefore vital to produce graduates with a fundamental understanding of the risk of an inefficient security strategy.

Research Approach

The research involves a single case centering on the development and implementation of an education programme. The research orientation is qualitative and reflexive. A grounded theory perspective is adopted, and an initial educational model incorporating security and knowledge created. An action research approach was adopted to guide the conduct of the case study. The intention is to further corroborate these factors and to elaborate the framework (Figure 1) as the research progresses.

Background To The Case - Masters in Business Studies

Many organizations in Ireland and worldwide are experiencing difficulties recruiting staff with the appropriate mix of business and technical skills to develop electronic business systems. The MBS (Elec-

tronic Business & Commerce) is the first of its kind in Ireland, and offers participants the opportunity to train for a career in the rapidly expanding electronic business sector. The programme provides participants with practical experience of electronic business strategies and technology, and will equip graduates with the skills, such as security, necessary to develop and exploit reliable electronic business applications.

Group Project

One of the core pedagogical features of the programme is a yearlong group project. It enables the students to apply all of the knowledge (explicit) gained through lectures and the skills necessary to apply the knowledge (tacit) gained to a relevant problem. Students are expected to form groups and develop a secure network to solve the IT requirements of a fictitious bank. Students, in groups of 6 are expected to generate a report outlining the security infrastructure of a fictitious bank. The bank will avail of Smart Card technology for both customers and (2000) employees. Students are also required to design the entire security and knowledge system in place, i.e. students are expected to provide a complete design of each layer of the banks network security, from the protocols used in network addressing to the physical procedures in place to protect the bank in question. Every type of organization aims to create knowledge, students should therefore also map the knowledge process within the bank and the security (map) in place to both share and protect it, baring in mind that the biggest risk is generally from within. Groups will also present their assessment of the environment outlined to a panel, independent of the other groups, they will then be expected to compare their proposed security network to an existing organization that will be identified at the presentation.

Constructing The Educational Model

The concept of risk management is not a new approach to security but a necessary strategy for any organizational infrastructure. Figure 1 outlines the complexity of the different types of networks and relationships that bind a case together, illustrating the diversity of both the internal and external environments. The component residing at the center of the diagram represents any case that competes with it's competitors through both collaboration and competition resulting in both beneficial lines of communication and threats to its security. Security, through policies and technology, is shown to be of equal importance to the knowledge that it is trying to protect. Knowledge should be shared to generate additional knowledge but also protected to provide a competitive advantage. The inverted rectangle, that encloses the case and its internal networks of knowledge workers, represents the value net of a typical organization. Co-opetition adds value to any firm, to create a valuable network, companies cannot operate in isolation; they must collaborate with customers, suppliers and even competitors (Brandenburger & Nalebuff, 1996) to create new, or expand existing markets. The top part of the net deals with customers and the bottom suppliers, the other players either complement or compete with the case. Complementors allow the case to expand and promote their market base through collaborating to share for example customer information or offer joint promotions. Due to the complexity of the interdependencies that exist a secure outer layer is necessary to both support and protect the integrity of the different networks and therefore the knowledge of the firm. The outer layer is represented by a continuous (arrows) process indicating that the steps related to both technology and the different actors within and externally are taken on an ongoing basis. The security plan and the IT used to support it is determined by management, who are responsible for controlling the changing policies that are needed to ensure that adequate monitoring and reactive strategies are enforced. Both the internal and external environment should be scanned and audited to determine any abuse or risk due to the different lines of communication created as a result of the relationships formed. If any risk is identified, it is then analyzed to determine the impact on the case and the strategy that should be used to prevent loss of knowledge. Once the risks have been evaluated they are then prioritized, the case's IT resources are evaluated and a plan created to combat the risk

(Greenstein et al., 2000). The plan itself should then be monitored through auditing its success to determine how the security strategy utilized can be improved.

Knowledge & Security

In order to create knowledge an organization or a university must collaborate with other organizations while still sustaining a competitive advantage (private knowledge). Therefore, it is essential to define the factors and barriers to expand the concept. The identification of these characteristics is necessary to implement a model to foster its creation. Thus, this section looks at eight factors proposed by the authors for both securing and sustaining knowledge creation. The factor/barriers are proposed to describe the characteristics of the educational model. Each of the dimensions identified are outlined as follows and will be addressed by each project group:

(1) *Impact on the Organization:* research is full of examples of the advantages associated with knowledge generation and utilization (Hertog & Huizenga, 2000). It provides the firm with the ability to target valuable markets and utilize their resources when their systems are fully integrated. However the firm must fully understand and provide a clear definition of what knowledge means to the organization in question to achieve a competitive advantage. Therefore, any organization that classifies itself, as a learning or knowledge environment is fully aware of implications of inadequate security. The difficulty, when cost isn't too high an issue, is the balance necessary in allowing groups (internal/external) and individuals to share information without being too lazed in protecting private (competitive) knowledge.

(2) *Structure / Culture:* the goals for any case can vary from sharply focused, where specific targets are required to a more general approach to knowledge creation. Cole (1992), states that knowledge "*has undergone extensive social negotiation of meaning.....*", in this instance a more laxed attitude to knowledge creation and use is tolerated as the organization has not yet invested in utilizing knowledge as a competitive advantage and are as a result laxed in their attitude in securing and promoting a knowledge culture. If management promotes knowledge and provides some type of motivation to its employees to collaborate, knowledge will be created. Additionally to be successful, security must be seen as equally important as the corporate knowledge it has been devised to protect. It must be taken seriously and every actor must be aware of the threats and risks of an insufficient security infrastructure.

(3) *Policies / Models:* are necessary guidelines in the creation of knowledge and the type of model followed can be a factor for, as opposed to a barrier to knowledge creation. The policies put in place by management provide the different actors with clear guidelines of what should be done to create a knowledge-driven environment and the rules governing external collaboration. However the polices governing knowledge must be enforced to be of any value as should the security policy implemented. Every organization develops security policies, but a number fail to follow the rules outlined to protect the integrity of the information that the model is trying to protect. To be successful a security model should be supported by management and each actor within should be fully aware of its existence and the necessity to consistently review it as risks are constantly changing.

(4) *Actors:* Checkland (1981) illustrated the importance of investigating the different actors and relationships within an organization for end-user acceptance of any system or methodology. If the internal actors and groups are not considered in the design of a knowledge driven organization or KMS it will fail to achieve its objectives. Employees need to be educated and motivated in the benefits of sharing and creating knowledge. If they are not the organization risks the loss of private knowledge in the form of their trained experts to the public domain (competitors). An organization's biggest asset is it's employees, however they are unfortu-

nately the biggest risk to the security of the group, department and therefore the organization in question. Employees need to receive security awareness training and should be motivated to follow whatever security policy that is in place.

(5) *Network Design / Group:* the structures of organizations differ from hierarchical to flat to virtual, however the number of levels and the trust between internal/external groups can dramatically affect the level of knowledge achieved. The greater the number of managerial levels the more complex the creation and dissemination process. The design of the communication network mimics the structure of the organization and the level of interaction in sharing knowledge between the different departmental teams. Technology automats manual processes with the objective to reduce human error (Kirwan, 1994) and increase productivity. Therefore, it can often be used to imitate an inefficient process instead of reengineering it. Communication networks, too, mirror the corporate structure and the groups that reside within. The design of a networks security, complements the divisions between groups and the trusted relationships established between particular domains. The technical design of a corporate network should allow groups to collaborate but also protect against any risks that could threaten the integrity of the knowledge stored.

(6) *Taxonomy of Knowledge Security:* Polanyi (1967) states that knowledge is commonly categorized as either explicit or tacit. Explicit knowledge refers to corporate terminology, procedures and fact-based material (Walsh & Dewar, 1987), which are easily created and maintained as it, isn't dependent on specific knowledge workers or experts. However, if the goal of the case is to utilize and create tacit knowledge the organization relies on its internal actors or human assets and therefore their expertise (Grant, 1996). Thus the type of knowledge collected by the organization dictates the complexity of the process of transferal and the level of security needed to support the corporate goal.

(7) *Technology:* is the central component that binds both security and knowledge together. Both factors are dependent on technology to facilitate their operational characteristics as dictated by the firm. Knowledge and security can be traced back to their core components by mapping the technology necessary to support each. *Knowledge & Security Mapping*: are basically a means of tracing the different pieces of the puzzle and the dependencies of the different devices or steps necessary. Mapping allows a company to identify the different ingredients in the creation of knowledge and the technology or policies necessary to both protect and enable its production.

The combination of the three blocks or components, outlined in figure 1, allowed a thorough investigation of both security and knowledge. The construction of the model (see Figure 1) provides students with a guide for the collection of the necessary data to piece together a picture of the case and the overall impact of security on the communication (knowledge) network. The statement of the research objective, as outlined in section 3.0, is complex. The qualitative analysis of the study will validate the steps as presented in the model. The goal of the study resides in the integration of the three factors, identified by the researchers, which influence knowledge creation and security and as a result ultimately learning.

Proposed Presentation

The presentation would focus on the operationalization of the educational framework as discussed and depicted in Figure 1. While the research is at an early stage, some preliminary lessons have been learned, and these would be reported. For example, the inter-relationship that exists between security and knowledge is extremely complex even interdependent Additional from a pedagogical perspective the advantage of enabling students to gain some tacit knowledge of the area through the design of a se-

curity network as well as the comparison of one design to another. This will be investigated further in, as the research progresses; the results of the project will be presented at the conference.

References

Adam, F. (1992). *The identification and analysis of information flows among senior executives – An empirical study*. Masters Thesis.

Adam, F. (1999). *An empirical investigation of the information and decision networks of organizations and their implications for IS research*. ***Unpublished Manuscript.***

Argyle, M. (1994). *The psychology of interpersonal behavior* (5th Ed.). Penguin, Harmondsworth.

Avison, D.E & Fitzgerald, G. (1995): *Information systems development: methodologies, techniques and tools*. (2nd Ed.). McGraw-Hill.

Brandenburger, A.M., & Nalebuff, B.J. (1996). *Co-opetition*. Doubleday

Baron, R.A. & Byrne, A.. (1977). *Social psychology understanding human interaction* (2nd Ed.). Boston: Allyn and Bacon Inc.

Cantoni, F; Bello, M & Frigerio, C. (2001). Lowering the barriers to knowledge transfer and dissemination: the Italian cooperative banks experience. *Global Co-operation in the New Millennium, ECIS, 2001*.

Cole, P. (1992). Constructivism revisited: A search for common ground. *Educational Technology* 32(2), pg27-34.

Connolly, T., Begg, C., & Strachan. (1996). *A database systems: A practical approach to design, implementation and management*. Addison-Wesley.

Driscoll, M. (1998): *Web - based training: using technology to design adult learning experiences*. Jossey-Bass Pfeiffer.

Drucker, P. (1993). *Post-capitalist society*. New York: HarperCollins.

Entwistle, N. (1988). *Styles of learning and teaching: An integrated outline of educational psychology for students, teachers and lecturers*. London: David Fulton.

Goldman, J.E. (1998). *Applied data communications: A business-oriented approach*. John Wiley & Sons, Inc

Gollmann, D. (1999). *Computer security* John Wiley & Sons.

Grant, R.M. (1996). The Resource-based theory of competitive advantage: Implications for Strategy Formulation. *California Management Review*.

Greenstein, M. & Feinman, T.M. (2000). *Electronic commerce: Security, risk management and control*. Boston: Irwin McGraw-Hill.

Hertog, J.F. & Huizenga, E. (2000). *The knowledge enterprise, Implementation of intelligent business strategies*. London: Imperial College Press.

Huczynski, A., & Buchanan, D. (1985). *Organisational behaviour* (2nd Ed.). Kidlington, Oxon: Prentice Hall International.

Jonassen, D.H., & Reeves, T.C. (in press). Learning with technology: Using computers as cognitive tools. In D. Jonassen (Editors) *Handbook of Research on Educational Technology*. NY: Macmillan.

Johnson, D., & Johnson, R. (1990). Cooperative learning and achievement. In S. Sharon (Editor), *Cooperative Learning Theory and Research*, pp. 22-37. NY: Praeger.

Kyllonen, P.C., & Shute, V.J. (1989). A taxonomy of learning skills. In P.L Ackerman, R.J. Sternberg, and R. Glaser (Editors), *Learning and Individual Differences: Advances in Theory and Research*, pp. 117-163, NY: W.H Freeman and Company.

Laudon, K.C. & Laudon, J.P. (2000). *Management information systems: Organization and technology in the networked enterprise*. Prentice-Hall.

Lebon, G. (1986). *The crowd – A study of the popular mind*. London: Fisher Unwin.

McGrath, J.E. (1984) *Groups: Interaction and performance*. New Jersey: Prentice-Hall.

McCormack, C. & Jones, D. (1997). *Building a Web - based education system*. JohnWiley & Sons, Inc

Panko, R, (2000). *Business data communications & networking*. Prentice Hall.

Powell, P., Loebbecke, C., Levy, M. (2001). SMEs, Co-opetition and knowledge sharing: The IS role. *Global Co-operation in the New Millennium, ECIS*, 2001.

Rutkowski, M. (1999). *Two perspectives on knowledge transfer*. Retreived from the Web at http://www.walshcol.edu/mrutkow/knowledgeA.htm

Stallings, W. (2000). *Business Data Communications*. Fourth Edition, Prentice Hall.

Tiwana, A. (2001). *The knowledge management toolkit: Practical techniques for building a knowledge management system*. Upper Saddle River, NJ: Prentice Hall.

Wells, R.A. (1992). *Computer –mediated communication for distance education: An international review of research monographs 6*. American Center for the Study of Distance Education, State College, PA, Pennsylvania State University.

Wernerfelt, B. (1984). A resource based view of the firm. *Strategic Management Journal*.

Whiteley, D. (2000). *E-Commerce: Strategy, technologies and applications*. Wiley.

Biography

Karen Neville holds both a Masters of Science in Management Information Systems and a Bachelor of Science in Business Information Systems from University College Cork, Ireland where she is employed as a College Lecturer. She is currently registered as a PhD student, under the supervision of Professor Philip Powell, at the University of Bath, UK. Her publications, to date, include papers focusing on ICT initiatives, E-Learning and Educational Systems that have been published in some of the top information systems conferences and journals. However the focus of her research has now expanded to incorporate the areas of Knowledge Management and Security.

Philip Powell BSc, PhD, MBCS, CITP, MILT. Philip Powell is Professor of Information Management and Director of the Center for Information Management at the University of Bath. Formerly, Professor of Information Systems, University of London and Director of the Information Systems Research Unit at Warwick Business School. Prior to becoming an academic he worked in insurance, accounting and computing. He is the author of four books on information systems and financial modeling including *Management Accounting: A Model Building Approach, Information Systems: A Management Perspective* and *Developing Decision Support Systems for Health Care Management*. He has published numerous book chapters and his work has appeared in over seventy international journals and over 100 conferences. He is Managing Editor of the Information Systems Journal, Book Reviews Editor of the Journal of Strategic Information Systems, and on a number of other editorial boards. He is president of the UK Academy for Information Systems. He serves on the Alliance for IS Skills steering group.