December 2003

Knowledge and Security

Karen Neville
University College, Cork

Philip Powell
University College, Cork

Niki Panteli
University College, Cork

KNOWLEDGE AND SECURITY

Karen Neville
University College, Cork
kneville@afis.ucc.ie

Philip Powell
University College, Cork

Niki Panteli
University College, Cork

Abstract

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. However, collaboration can, if not managed and controlled effectively become a threat to security. Organizations with the ability to protect valuable knowledge have many incentives to do so. This research investigates the interactions of security and knowledge to develop a model to research success and failure factors. 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. Examples from an on-going case illustrate use of the model.

Keywords: Knowledge, security and information technology

Introduction

Security of corporate assets is more complex as knowledge becomes a key organizational resource. The literature is replete with examples of security models and policies that provide guidelines for the protection of information [Stallings, 2000] that may be inadequate for knowledge. However, the information economy has resulted in virtual communication networks and groups collaborating and competing to create knowledge and competitive advantage [Brandenburger and Nalebuff, 1996]. These relationships allow individuals and organizations to interact with new partners such as competitors and suppliers to expand their knowledge bases. Knowledge workers or virtual groups with a common goal can form virtual relationships to generate tacit and explicit knowledge.

Traditionally, security has been concerned with the protection of assets. Valuable information has always been guarded in order to retain its worth and provide advantage over a competitor. The increasing value of knowledge means that the complexity of security solutions needed to guard corporate secrets has increased [Bishop *et al.,* 1997].

This paper develops a model to support the investigation of the inter-relationship between security and knowledge. The research outlines factors and barriers to effective security and knowledge creation. Security must be sufficient to protect an organizations knowledgebase but not to restrict the process. A secure environment is necessary to create knowledge but knowledge of security is necessary for the provision of a secure environment.

Theoretical Foundation

Knowledge

Knowledge is a complex resource, "*knowledge is a fluid mix of framed experience, values, contextual information, and expert insight...In orgnizations, it often becomes embedded not only in documents or repositories but also in organizational routines,* *processes, practices and norms"* Davenport & Prusak, (1998). Knowledge exists within the actors of the firm, making them a valuable asset [Avison & Fitzgerald, 1995]. As a result a major risk lies in preserving this knowledge, without doing so the knowledge accumulated cannot be duplicated or made available to less experienced practitioners [Hertog & Huizenga, 2000]. Organizations face the dilemma of protecting knowledge from internal and external risks. Knowledge is acquired through internal and external relationships. Groups internally cooperate to achieve a common goal, and externally mutually beneficial relationships are formed [Neville et al., 2002]. Information is gathered through these communication networks cooperating and competing to possess useful knowledge. Organizations must therefore manage risks in an open network. Knowledge transfer has extended from passing information from individual to individual [Cantoni et al., 2001] to moving knowledge around the organization (or virtual organization) or to another [Rutkowski, 1999]. However problems of knowledge creation arise due to lack of education, employees leaving, and a lack of internal collaboration resulting in duplication of work or internal competition. These arise due to a lack of management of the communication network or a strict security strategy preventing individuals from knowing what another is doing. Co-opetition, simultaneously co-operation and competition, involves the sharing of knowledge to gain competitive advantage [Powell et al, 2001]. Individuals collaborate to combine knowledge and create new knowledge to innovate. However this type of collaboration or sharing of knowledge can be exploited for competition.

Security

Security encompasses making information systems safe from risks without reducing the productivity of employees [Goldman, 1998]. Security research focuses primarily on risk analysis, checklists and evaluation. Checklists help to outline the technologies needed to accomplish the requirements of end-users. Traditionally, checklists identify security controls that should be implemented on computer-based systems. But they are used as procedural requirements for implementation without examining the implications of the risk regarding knowledge or culture [Dhillon & Backhouse, 2001].

The first step in securing knowledge is to examine potential threats from the internal and external environment. Once threats have been identified resources are needed to combat them - risk management and evaluation, though a successful security policy needs to be proactive [Goldman, 1998]. A security strategy is needed to protect knowledge and data resources [Castano *et al.,* 1994]. Security goes hand in hand with dependency and any organization that implements widespread IS 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 [Whiteley, 2000]. The main tasks involved in developing a security model to protect the corporate knowledge-base are, first avoiding or reducing the risks through both internal and external countermeasures (provision of an effective security strategy and culture), and second contingency planning.

Security can hinder and enable collection of data, information retrieval and knowledge creation. The complexity of knowledge and security is undeniable and the two are intertwined. Security is a vital component in the creativity of a competitive environment. The reliance of knowledge management and creation on existing and future interrelationships is evident yet difficult to validate. An organization is viewed as a collection of relationships and knowledge gained as a result [Tiwana, 2001]. Large organizations with the ability to protect valuable knowledge have incentives to be innovative and therefore remain competitive even in co-opetition. Technology binds security and knowledge together. Organizations use technology to collect and share knowledge, while simultaneously protecting it.

Technology

Alavi and Leidner (1999) argued that the importance of knowledge is based on the hypothesis that the barriers to the transfer and duplication of knowledge award it with enormous strategic importance. Organizations use IT to develop systems that can collect and manage knowledge. A knowledge base reduces the level of experience needed by managers and improves decision effectiveness. A '*true'* knowledge base will allow the acquisition of experience of experts to reduce the loss should the employee leave. Secure protocols, standards and encryption can protect communication networks and devices such as firewalls and secure routers filter out possible threats. However, network security and access controls to control internal users is useless if the organization is devoid of the actors necessary to promote a culture of security awareness and knowledge to limit the threats posed [Goldman, 1998].

Research Objective

Given the importance of security and knowledge, it is vital that organizations understand their interaction. This research constructs and implements a model to assist understanding of the inter-relationship. An additional goal is to investigate the barriers to the successful implementation. The research investigates security in virtual teams as a factor in the creation and management of knowledge. Actors combine to form groups, groups merge to form departments, and ultimately virtual partnerships and competitors. Relationships, internal and external, can hinder and foster knowledge. A security strategy can dictate, frustrate and protect this fragile network and result in a trade-off between security and productivity.

Research Approach

The research context is that of a single case organization. The research orientation is qualitative and reflexive. A grounded theory perspective is adopted, and an initial framework incorporating security and knowledge created.

The case firm, Practical Solutions Limited (PSL), founded in 1999, as a virtual firm, links graduates with a range of technical skills to satisfy the demand for part-time consultancy. PSL's business model is based on linking knowledge workers to firms wishing to outsource the development of on- and off-line systems. It displays a rare combination of technical innovation and commercial awareness. Currently, the staff consists of twelve knowledge workers offering practical experience and skills acquired from their full-time positions. A primary source of development projects is on-line education systems used to develop employee skills. Success is based on communication with external groups collaborating to produce software solutions. PSL is built on a technological foundation, using technology to facilitate the communication and to match skills with requirements. Each contractor participates on a part-time basis and utilizes the knowledge (tacit and explicit) gained from their current positions to solve another, possibly a competitor's, IT problems. PSL uses a network of contacts by email and the web, in the form of discussion forums, to match a suitable developer to a problem. The case represents one of the biggest organizational security risks, an employee sharing knowledge for personal gain.

Research Model

Figure 1 outlines the complexity of the different types of networks and relationships that bind an organization together, illustrating the diversity of internal and external environments. The central components represent an organization case that competes through collaboration and competition, resulting in beneficial communication and threats to security. Knowledge should be shared to generate additional knowledge but protected to provide a competitive advantage. The inverted rectangle that encloses the organization and its internal networks of knowledge workers represents its value net. The upper part of the net deals with customers and the lower, suppliers, the other players complement or compete. Complementors allow the organization to expand and promote their market-base to share customer information or offer joint promotions. A secure outer layer is necessary to support and protect the integrity of the different networks and the knowledge. The outer layer is represented by a continuous process. The security plan and the IT support is determined by management who are responsible for the policies needed to ensure adequate monitoring and reactive strategies. The internal and external environment are scanned and audited to determine abuse or risk. If a risk is identified it is analysed to determine the impact and the strategy to prevent loss of knowledge developed. Once risks are evaluated they are prioritised, IT resources are evaluated and a plan created to combat the risk.

Knowledge and Security

The need to share knowledge internally and externally suggests a paradox in that in order to create knowledge the firm must collaborate with others (public knowledge) while sustaining competitive advantage (private knowledge). This section identifies a set of factors for securing and sustaining knowledge creation.

(1) *Organizational Impact:* knowledge generation and utilization provides the firm with the ability to target valuable markets. However the firm must understand its knowledge assets to achieve competitive advantage. Yet a learning environment has implications for security. The difficulty is the balance necessary in allowing groups (internal/external) to share information without endangering private (competitive) knowledge.

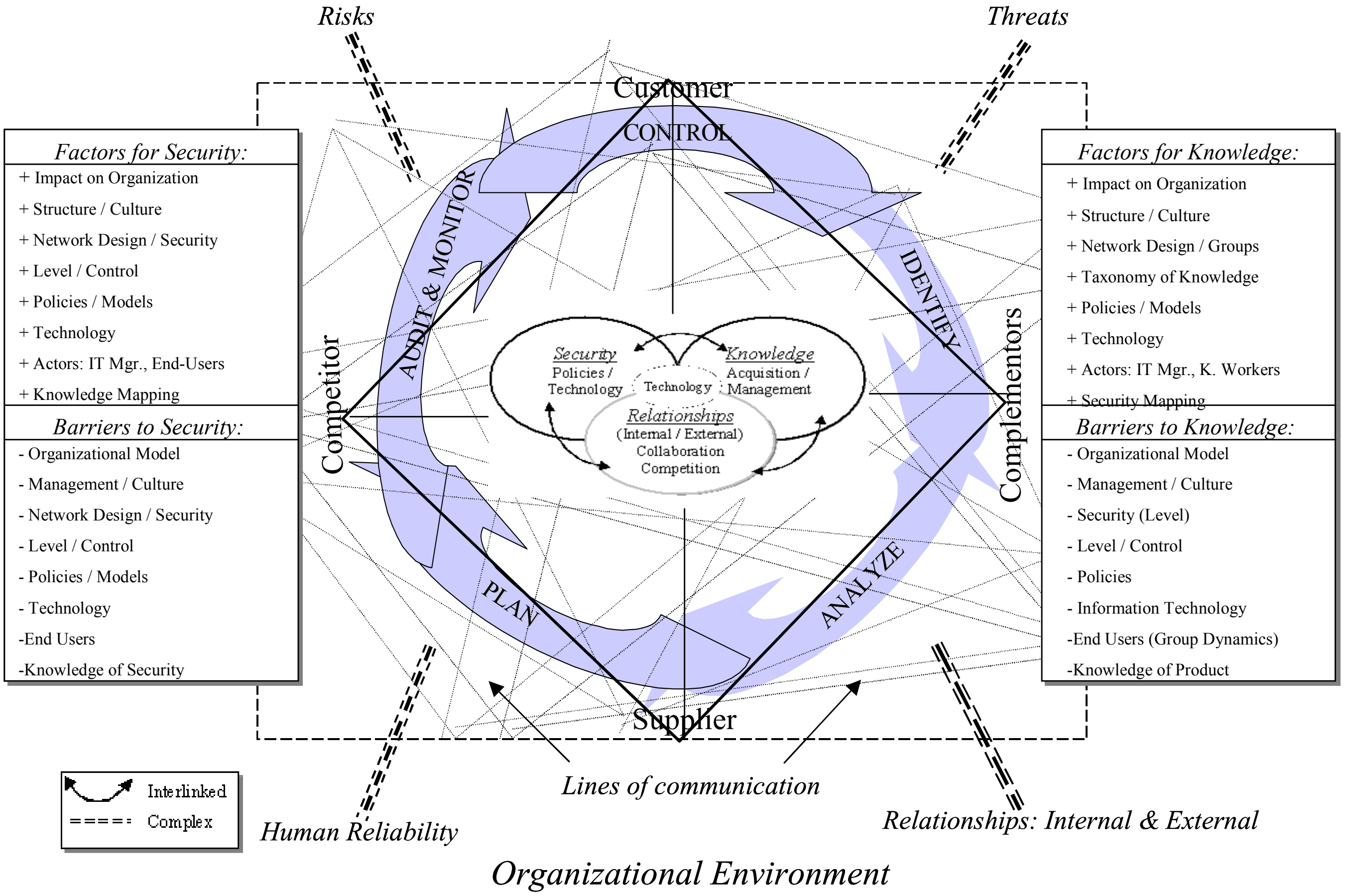

Figure 1. The Research Model

(2) *Structure/Culture:* Researchers have [Hertog & Huizenga, 2000], acknowledged that knowledge has undergone extensive negotiation of meaning. If management promotes knowledge and motivates employees to collaborate, knowledge will be created. Security must be seen as important as the corporate knowledge it protects.

(3) *Policies/Models:* are guidelines in the creation of knowledge. Policies provide actors with guidelines to create a knowledge-driven environment and the rules governing external collaboration. However, policies must be enforced.

(4) *Actors:* If actors are not considered in the design of a knowledge-driven organization it will fail. Employees need to be educated and motivated in the benefits of sharing and creating knowledge. If they are not, the organization risks loss of private knowledge. Employees need security awareness training and to be motivated to regard security as important.

(5) *Network Design/Group:* the hierarchy and trust between internal/external groups can affect knowledge. The greater the managerial levels the more complex the creation and dissemination process. The communication network mimics the structure and the interaction in sharing knowledge between teams. Technology is often used to imitate inefficient processes. The design of network security complements the divisions between groups and the trusted relationships established. The technical design of a corporate network should allow groups to collaborate but protect against risks that could threaten the integrity of knowledge.

(6) *Taxonomy of Knowledge Security:* if the goal is to create tacit knowledge the organization relies on internal actors and their expertise. Thus knowledge type dictates the complexity of the process of transferal and the security required.

(7) *Technology:* binds security and knowledge together.

(8) *Knowledge & Security Mapping*: are a means of tracing the dependencies. Mapping allows identification of the different ingredients in the creation of knowledge and the technology or policies necessary to protect and enable its production.

Conclusions

This paper focuses on the inter-relationship between two dependent factors: security is needed to both create and protect knowledge and if security is to be successful every actor within the case must be aware or possess the knowledge necessary to identify and control any risk. The research outlines the factors necessary for the successful implementation of both security and knowledge.

References

Alavi and Leidner [1999] Knowledge Management Systems: Issues, Challenges and Benefits, Communications of the Association for Information Systems, Volume 1, Article 7.

Avison, D.E and Fitzgerald,G [1995] Information Systems Development: Methodologies, Techniques and Tools, Second Edition, McGraw-Hill Companies.

Bishop M, Cheung S & Wee C [1997] The threat from the net (Internet security). IEEE Spectrum 34: 56-63.

Brandenburger, A.M., and Nalebuff, B.J., [1996] Co-opetition, Currency Doubleday

Cantoni, F; Bello, M & Frigerio, C., "Lowering The Barriers To Knowledge Transfer and Dissemination: The Italian Cooperative Banks Experience", Global Co-operation in the New Millennium, ECIS, 2001.

Castano, S., Fugini., M., Martella, G., Samarati, P., [1994] Database Security, Addison-Wesley, Publishing Company, ACM Press.

Davenport, T.H., & Prusak, L., [1998] Working Knowledge, How Organizations Manage What They Know, Harvard Business School Press

Dhillon, G., & Backhouse, J., [2001] Current Direction in IS Security Research: Towards Socio-Organizational Perspectives, Information Systems Journal, Volume 11, Number 2.

Goldman, J.E, [1998] Applied Data Communications, Wiley Publishers.

Greenstein, M. & Feinman, T.M., [2000] Electronic Commerce: Security, Risk Management and Control.

Hertog, J.F. & Huizenga, E., [2000] The Knowledge Enterprise, Implementation of Intelligent Business Strategies.

Neville, K., Adam, F. & McCormack, C., [2002] Mentoring Distance Learners, Proceedings of the Xth European Conference on Information Systems.

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, **http://www.walshcol.edu/mrutkow/knowledgeA.htm**.

Siegel, J, Vitaly K, and McGuire, A., [1986] Group Processes in Computer-Mediated Communication, Organizational Behaviour and Human Decision Processes, 37.

Stallings, W., [2000] Network Security Essentials, Application and Standards, Prentice Hall, Inc., New Jersey.

Tiwana, A., [2001] The Knowledge Management Toolkit, Upper Saddle River, NJ: Prentice Hall.

Whiteley, D., [2000] E-Commerce: Strategy, Technologies and Applications, Whiley Publishers.