

Human Issues in Secure Cross-Enterprise Collaborative Knowledge-Sharing:

A Conceptual Framework for Understanding the Issues and Identifying Critical Research

Ann Majchrzak¹

Center for Telecommunications Management
Professor of Information Systems
Marshall School of Business
University of Southern California
Los Angeles, CA 90089
majchrza@usc.edu

April 15, 2004

¹ I would like to thank the following individuals who helped in the development of this white paper: Omar El Sawy, Sirkka Jarvenpaa, Bob Carman, Vern Lott, Kevin Kobelsky, Dan O'Leary, Rob Shively, Susan Maraghy, Charlie Meister, Morley Winograd, and Bill Boni. This research was funded by the Department of Homeland Security, Directorate of Information Analysis and Infrastructure Protection.

Human Issues in Secure Cross-Enterprise Collaborative Knowledge-Sharing: A Conceptual Framework for Understanding the Issues and Identifying Critical Research

Table of Contents

Executive Summary

1.0 Problem Statement

2.0 Overview of Approach

3.0 Collaborative Knowledge-Sharing as an Emergent Process

4.0 Individual-level Factors that Reduce the Probability of Information Security Breaches
in Collaborative Knowledge-Sharing

5.0 Implications for Organizational-Level Facilitators for Promoting Security in
Knowledge-Sharing

6.0 Summary of Organizational-level Facilitators

7.0 Implications for Research

8.0 Conclusion

9.0 References

Human Issues in Secure Cross-Enterprise Collaborative Knowledge-Sharing: A Conceptual Framework for Understanding the Issues and Identifying Critical Research

Executive Summary

This white paper is addressed to personnel at the Department of Homeland Security interested in understanding the human issues underlying security breaches in cross-enterprise collaboration, with particular emphasis on the private sector. Cross-enterprise collaboration requires simultaneously allowing rich discussion while, paradoxically, providing maximal information security. Current approaches to information security do not effectively manage this paradox, in part because there is a lack of appreciation for the emergent nature of both the collaborative knowledge-sharing process and the decision to commit a security breach. Emergence suggests that the exact nature of the trade-offs between sharing and security experienced by an individual engaged in the collaborative process cannot be known in advance. Thus, policies and procedures that specify how an individual should act are both infeasible and likely to be ignored.

Emergence during the collaborative process suggests that information security policies should emphasize keeping employees dynamically informed about potential security breaches that may result from actions they take, rather than prohibiting certain types of sharing or certain types of actions. Emergence also suggests that any security protection tool, policy, or procedure must be self-deploying and seductive, meaning that it must draw people into “doing the right thing”, sometimes without ever realizing it.

Emergence also implies that leaders of an emergent process are rarely appointed, instead they emerge. Thus, leaders that champion information security protection need to be encouraged to emerge, rather than appointed. Emergence also means that knowledge relevant to information security breaches will be distributed across individuals within an organization and across organizations. There needs to be forums where information about breaches, fixes, and prevention can be shared. Finally, emergence suggests that people behave based on feedback rather than standard procedures. Thus, they need feedback on their work processes that encourage them to behave securely.

A conceptual framework for understanding how to manage emergence in the collaborative knowledge-sharing process to promote secure behavior is offered. The framework identifies precursors to collaborative knowledge-sharing information security breaches and suggests organizational facilitators for reducing the probability of a breach. This framework suggests that appropriate organizational facilitators are focused not on prohibiting or requiring employee behaviors, but instead conform to the way employees collaborate with others outside the firm – a collaboration not intended to breach security. These facilitators include attending to the employee-firm psychological contract, tools that help employees understand the probable consequences of their behavior, development of security procedures and tools that are integrated into the work in a way that allow each individual to play a different leadership role in maintaining security, information security policies that address the very different security concerns expressed by the individual and group within the organization, and consciously adopting an information security strategy that is matched to the firm's market position. This

conceptual framework is largely untested. Given the urgency of the need to ensure the nation's cyber security, this framework deserves focused research attention.

Human Issues in Secure Cross-Enterprise Collaborative Knowledge-Sharing: A Conceptual Framework for Understanding the Issues and Identifying Critical Research

1.0 Problem Statement

Any time two individuals at two different organizations share knowledge, there is the opportunity of an information security breach. Yet, collaboration across firms is becoming increasingly necessary in today's competitive marketplace. Private sector firms are finding themselves increasingly engaged in supply chain partnerships, co-development agreements, consortia, electronic marketplaces, and joint ventures. Individuals involved in these collaborations must conduct their business without breaching information security. As these types of cross-enterprise collaborations continue to grow in the private sector, the potential of information security breaches grows as well (Garg et al, 2003). Moreover, the increased use of the Internet as the primary means for collaboration makes the cyber security concerns of collaborative knowledge sharing particularly pressing.

Shih and Wen (2003) list ten threats to what they refer to as "E-Enterprise networks" (defined as networks that connect supply chain partners). These are identified in Table 1. We simplify their ten threats and focus on four areas of information security concerns.

The first, and most obvious information security risk is *Sharing the Corporate Jewels*. The concern here is that knowledge that executives believe represent corporate secrets are offered by the firm's employees to the collaborative partner. By sharing that knowledge, the competitive advantage that the firm had by keeping that knowledge secret has now been harmed. This may occur informally through conversations or by sharing documents that the firm would have preferred to have remained secret. The conflict between General Motors and Volkswagen involving the alleged theft of intellectual property, including numerous designs and trade secrets, is a case in point. The leak of code for Microsoft's Windows 2000 and Windows NT 4.0 is another example of corporate jewels being inappropriately shared (Menn, 2004).

Table 1: Shih & Wen's (2003) Most Likely Threats on E-Enterprise Networks

Networks	Communicati	Attack	Most Likely Threats to E-Enterprise (note)											
			1	2	3	4	5	6	7	8	9	10		
Internet	B2C	Outsiders	X	X		X								
Extranet	B2B	Business	X	X	X	X				X	X			
Intranet	E2E	Insiders	X	X	X	X	X	X	X	X	X	X	X	X

Note: Most Likely Threats (1-10) to the E-Enterprise is defined as follows:

Natural Hazards

- (1) Natural Hazards or disasters that may interfere with business operations or enterprise information systems, such as floods, fires, earthquakes, hurricanes, and storms

Human Hazards

Intentional/Malicious Threats

- (2) Unauthorized access to Web sites, information systems, and propriety intellectual assets
- (3) Misuse of authorized access to Web sites, information systems, and propriety intellectual assets
- (4) Intentional tampering or demolition of organization information
- (5) Intentional physical intrusion of business operations or enterprise information systems
- (6) Physical theft

Unintentional Threats: Human errors, omissions, ignorance, etc.

- (7) Unintentional alteration of organization information
- (8) Unintentional demolition of organization information
- (9) Unintentional physical intrusion of business operations or enterprise information systems
- (10) System or computer failure

A second concern related to information security risk is *Granting Unauthorized Access*. This concern arises when, during the collaboration, the employee allows members of the partner organization access to explore proprietary or confidential information. This may occur by providing individuals from the partner organization access to the firm's portal, use of one's password, or the ability to visit the premises unescorted. One example of this provided by an industry executive was the case of an employee with restricted access privileges sharing his password with a member of the

partner organization so that the member could look at certain files. While the member did not misuse this privilege, according to the executive, this action by the employee essentially defeated the security system, exposing the system to higher risk. Allowing temporary employees access to corporate information after the employee's services are no longer needed is another example of such a threat (Champlain, 2003). Competitive intelligence, corporate espionage, and now terrorist information gathering is often pursued through unauthorized access (Erickson et al, 2003; Rothke, 2001).

A third concern related to information security in collaborative knowledge sharing is what we call *Not Following Security Procedures* during collaboration. This is a concern common across all work environments – whether collaborative or not: that of failing to take proper precautions to prevent unknown others from accessing the organization's knowledge (e.g., failing to change passwords often, logging on remotely in insecure environments, leaving sensitive documents around for others to see, leaving a machine logged-on yet unattended, and using unlicensed software). For collaborative environments, not only must the focal firm follow security procedures, but assurances that partner organizations are following these procedures are needed as well. Champlain (2003) describes the case of an application service provider who failed to encrypt password files, harming the client firm's reputation. An industry executive described how a supplier failed to follow proper information protection procedures, leaking client confidential information to a competitor.

A final concern is *physical intrusion*, in which hackers or cyber terrorists are able to access information either because of bugs in software programs, inadequate security measures written into the code, or users unintentionally providing hackers with confidential information in the course of their everyday actions. In the experience of one security research consulting firm, most organizations still fail to use encryption for their cross-enterprise email, allowing hackers to view in plain text internal memos as well as learning information about the network typology and service level that can be used for a later attack. Internet discussion and chat groups are often the targets of such intrusions. One technique is for the perpetrator to join a List Server (e.g., distribution list of people interested in a similar topic). Joining returns a list of all other subscribers, as well as providing access to archived and searchable technical discussions. According to the Air Force, foreign intelligence agents use these chat rooms to spot experts, the labs they belong to (based on their email addresses), and information about the expert that could be exploited (such as marital affairs, indebtedness, or job dissatisfaction). They use this information to ultimately recruit the expert as an “insider” with access to confidential information the agent wants. Additionally, foreign nationals using multiple aliases have been observed to actively seek information in a variety of chat rooms on defense contractor research efforts that, once obtained, was passed to a foreign chat room in their native language.

These problems have become increasingly of concern as supply chains are increasingly connected through Internets, intranets, and extranets. “Since the partners are physically located at different geographic places, a networked computing environment is

indispensable for facilitating communications, collaboration, and resource-sharing, creating higher risk of attacks and vulnerabilities to security breaches” (Garg et al, 2003, p. 41). Moreover, while E-business requires that the Internet be safe and secure, “the reality is drastically different. Various economy-wide surveys reveal that between 36 and 90% of organizations reported computer security breaches in 2002. Concerns over security continue to be listed as a top challenge, hindering the multibillion dollar potential of B2B and B2C opportunities” (Garg et al, 2003, p. 23).

To avoid these concerns of security breaches, the traditional approach is to create policies that give employees the responsibility for avoiding a breach and to provide some security technology (e.g., firewalls) to make breaches more difficult. The policies inform employees of the actions expected of them when sharing knowledge with others (or when doing any work at all). The employee is given the responsibility to change passwords often, to not give others access to a database without informing systems administrators, to not share corporate secrets, to turn off a computer when not in use, to shred documents, to regularly remove the cookies from the hard drive, to take notice of others’ suspicious behaviors, and to be given strict instructions about which documents and knowledge can and cannot be shared with others. This traditional approach has been found to not work (Schlarman, 2001). Employees still pursue their own agendas, often with wanton disregard of security measures: they find these measures to get in the way, create additional burden for them in their jobs, and otherwise make the task of collaboratively sharing their knowledge with others that much harder.

A focus on policies that prohibit and restrict behaviors has led to what can be called *overzealous security administration*. Rarely discussed in Information Security circles, this traditional approach has often led to overly broad security policies that end up harming the collaborative process by reducing the timeliness with which information can be shared, and the give-and-take between collaborating parties to build trust. One industry executive reported that his firm was so “overzealous” about knowledge protection that knowledge sharing between business units was virtually non-existent. One business unit consistently withheld internal data on competitive assessments from the other business unit. When knowledge cannot be shared with external or internal parties – or cannot be shared without extensive and delayed review - decision-making slows down and thus timeliness with which an opportunity can be leveraged is lost. Additionally, when the sharing of knowledge is limited to pre-cleared documents, knowledge integration among the collaborative parties can be harmed. This problem has been identified, for instance, in the current frustration with information sharing among participants in DHS’s ISACs.

In this paper, we do not take the approach of suggesting yet more burdensome security policies to be followed by employees. *Instead, in this paper, we examine the precursors to information security breaches when employees are collaboratively sharing knowledge. We suggest that instead of dictating more security measures that users must conform to, organization and business processes must be redesigned to conform more closely to how an employee collaborates with others outside the firm – a collaboration not intended to breach security.*

2.0 Overview of Approach

Few holistic security views have been applied to business partners in cross-enterprise collaborations. Most views have approached the problem through discrete incongruous security control practices (Shih & Wen, 2003). Champlain (2003) relates a case in which security policies were actually in conflict across firms, and even within the same organization.

A holistic approach then is one that looks at the collaboration not as discrete events, but as an integrated process. In this paper, we view collaboration and threatened security breaches as part of a work process. This work process is not predictable and thus cannot be managed or controlled like a routine process. Moreover, central to the collaborative work process is the individual. As such, then, we focus in this white paper on the individual: the motivations, constraints, and relationships that impact how an individual behaves in situations where security breaches during collaborative knowledge sharing are possible.

Our analysis of the individual helps to elaborate in detail the paradox faced by the individual in a collaborative knowledge-sharing situation. That paradox is for the individual to decide how to share and gain the right knowledge, without sharing and gaining the wrong knowledge. That is, as the individual engages a partner in

collaboration, the knowledge gained must increase the collaborative value, without also increasing corporate vulnerabilities.

How an individual manages this paradox is central, we argue, to understanding when and why security breaches will arise. Our conceptual framework, then, is designed to elaborate factors that help to explain how individuals manage this paradox.

This paper proceeds by first describing a view of the collaborative knowledge sharing process as essentially unpredictable. Then, we present factors that affect information security breaches during this process. Finally, we use these factors to identify the organizational levers needed to reduce the risk of security breaches.

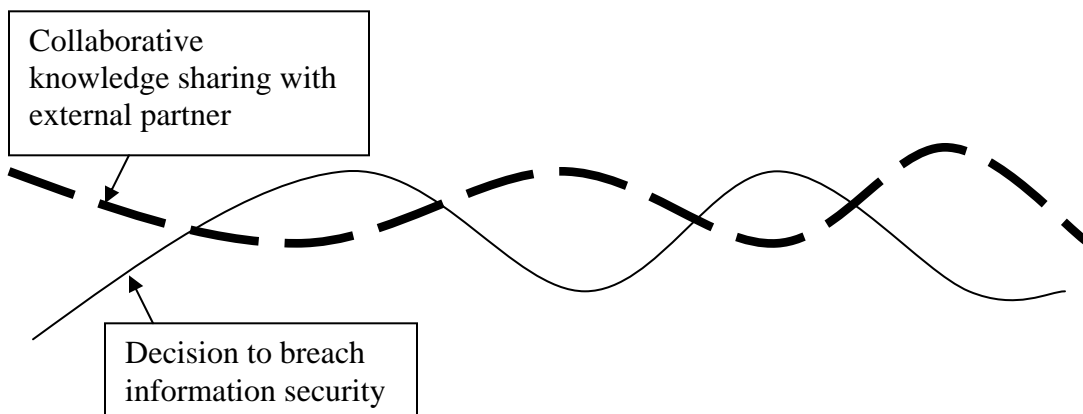
This conceptual framework is derived from existing theory, and enriched through anecdotes of security breaches. It has not been validated through empirical evidence. In fact, there is little research and documentation about the role of the individual in sharing knowledge in a way that maintains information security (Dervin & Shields, 1999). Thus our framework provides a focus for future research in this area.

3.0 Collaborative Knowledge-Sharing as an Emergent Process

Information security breaches during collaborative knowledge sharing can be conceptualized as two different work/decision processes that unfold over time, as

graphically depicted in Figure 1. The first process is the collaborative knowledge-sharing activity with the external partner: brainstorming, joint analysis, joint interpretation, and file sharing are common behaviors observed during collaborative knowledge sharing. The second process consists of those behaviors that put information security at risk. They include learning about corporate strategy, assessing what knowledge might be corporate jewels, learning what others in the organization might judge as sharing too much, identifying ways to provide access to files without granting unauthorized access, learning about security procedures, and deciding how to follow procedures without harming the collaborative process. Individuals engage in both processes simultaneously. When the processes suggest actions that are in conflict (as when access should be granted to an external partner to facilitate knowledge-sharing but can't because of access concerns), the individual must resolve a paradox.

**Figure 1: The two decision processes of Information Security breaches
During Collaborative Knowledge-Sharing**



A work process can be classified as routine when it is repeatable, or non-routine when it involves frequently varying inputs and processes, although with detailed analysis, could be structured to fit with the variations. But suppose a process could never be structured, no matter how much detailed analysis of the process was conducted. These processes have recently been referred to as “emergent” (Markus et al, 2002). Emergent work processes are those in which inputs and processes are unpredictable, and will remain so unpredictable that structured rules and procedures never completely apply. Often, strategic planning, organizational design, and revolutionary product development may unfold as emergent processes.

Table 2 depicts characteristics of emergent work processes. We argue that both processes – the collaborative knowledge-sharing process, and the decision to breach security – are emergent processes. In the second column of Table 2, we demonstrate the parallels between generic characteristics of emergent work processes and those of information security breaches in collaborative knowledge-sharing activities.

Table 2 Information Security Decision-making within Collaborative Knowledge-Sharing (CKS) as an Emergent Process

Characteristics of Generic Emergent Knowledge Processes	Characteristics of Information Security Decision-making within CKS
Problem deliberations, interpretations, and actions unfold unpredictably	Sharing of secret knowledge is a matter of interpretation; costs vs. benefits are situation specific and judgmental based on dynamics of CKS
Unpredictable user roles and work contexts	Users can play multiple roles throughout process; triggers for information security decisions unpredictable; autonomous decision-making with imperfect oversight
Difficult-to-share tacit knowledge is distributed across people and places	Information about what is secret, why, implications of sharing with external parties, which external parties are trustworthy collaborators, and which internal agents are high-risk is distributed and often tacit

First, in emergent knowledge processes, problem interpretations, deliberations, and actions unfold unpredictably. To collaborate securely often requires using judgment when defining what knowledge is secret. Moreover, costs and benefits are situation specific and judgmental, based on the dynamics of the collaborative knowledge sharing activity. In one example provided by an industry executive, the sharing of new product designs was highly situation specific in his firm: if the supplier was considered a “partner” and one where the expectation was of extensive future involvement, new product sketches would be shared in order to obtain valuable input. However, if future involvement with the supplier was in question, the same design information would be withheld and considered “sensitive”. Categorizing a supplier as a “future investment” versus “short-term investment” was a decision often made tacitly among a small group of

people. Therefore, as an individual is undertaking a collaborative engagement, the individual will need to make situation specific judgments about what is shareable and what shouldn't be.

Second, in emergent knowledge processes, the users and precise work contexts in which they find themselves are unpredictable (including when and why the process is performed, who's involved and which support tools are used). For information to be secure in collaborative knowledge sharing, collaboration often requires an inclusive rather than exclusive orientation. In ideal collaborations, individuals with special expertise are called in on the spur of the moment to provide their expertise; this reduces decision time, and speeds up the cycle of brainstorming (Majchrzak et al, 2000). The unpredictable nature of the experts needed makes it difficult to predefine access requirements. Moreover, the work contexts of the experts may change as well. One executive provided the example of a supplier that had been involved with the company for many years as a member of integrated product development (IPD) teams for defense contracts. At one point in the middle of the project, the supplier's parent company moved across the border, which had no apparent effect on the collaboration. However, the IPD team learned that the entire dynamics of the team process (such as sharing sketches) needed to change dramatically to conform to ITAR rules. It was easy for the team to forget that they were dealing with a foreign entity because locations of the individuals and expertise hadn't changed. Nevertheless, what was shared before would now be illegal.

Not only are there a range of people unpredictably involved in the collaborative knowledge-sharing, but the roles that people play when making decisions about information security will vary over time and situation. People can play one of three roles related to information security: perpetrator, bystander, or conspirator. The three roles are depicted in Table 3. The perpetrator personally decides to commit a security breach by sharing the knowledge, granting access, or failing to follow security procedures. Because the process is an emergent one with multiple interpretations about what is in fact a security breach, a perpetrator – even an intentioned one – is often a highly ethical person with strong values and a clear sense of right and wrong. Often the emergence of the process creates the possibility of a possible breach, not the individual. For example, one executive reported that a business process consultant from one firm was invited to spend a day with another firm to help with business process redesign for their procurement process. During the course of the day as the procurement process was analyzed for exceptions, it became increasingly clear that subcontractors used by the firm were also used by the consultant’s firm. The executive reported that the consultant returned and reported that he couldn’t talk to him “He knew information he didn’t want to know. If the information obtained about subcontractors had been leaked, there could have been lawsuits. We were invited in and shouldn’t have. But we didn’t know it at the time”, reported the executive. Clearly, the other firm was the perpetrator; but it would have been hard to predict this in advance.

The second role is that of the bystander. The bystander allows others to breach information security by not interjecting or reporting the incident. Observing a coworker

leaving her safe open and unattended is an example of a security breach. Allowing a colleague to share her password with someone else is also a bystander.

Finally, the third role is that of the conspirator. A conspirator makes it possible for others to commit breaches. For example, a conspirator may provide a partner with access to some documents, ignoring the fact that the access allows the partner firm the ability to obtain other documents of a more sensitive nature. An individual who fails to turn off their home computer allowing it to be used for virus attacks is a conspirator as well.

Table 3: Dynamically Changing Roles of Individuals as they Make Decisions Impacting Information Security

Role	Intention	
	Premeditated/Intentioned	Opportunistic/Unintentional
Perpetrator		
Bystander		
Conspirator		

An individual may undertake these three roles either intentionally (often premeditated) or unintentionally (often opportunistically). Research on betrayal of trust (Elangovan and Shapiro, 1998) characterizes these violations not as impulsive acts, but

rather the result of a cognitive decision process. When the decision is made before an opportunity arises, it is considered premeditated; when the decision is made in response to the situation, it is considered an opportunistic violation. Training programs and security policies tend to focus on avoiding premeditated intentions; moreover, most research has been focused on the type of “criminal” behavior that results from premeditation. However, by suggesting that the opportunities for committing security breaches cannot always be predicted, much security breach behavior will be opportunistic. This suggests, then, that people may play three different roles opportunistically as the collaborative knowledge process unfolds. Organizational levers for ensuring that these opportunistic decisions are made in the best interest of the firm are needed.

Finally, in emergent knowledge processes, knowledge is distributed across many different people who are brought together in local design activities, involving significant tacit knowledge that is difficult to share. In collaborative knowledge-sharing, determining what should be kept secret is often a combination of understanding the corporate strategy, understanding other projects that employees are working on, understanding other relationships that the firm may have had with this partner previously, etc. None of this knowledge is known by one individual. Thus knowing what knowledge should be withheld from that partner at any point in time is distributed across many different people.

As one example, one industry executive reported that, in the spirit of identifying complementary core competencies in a collaborative relationship with another firm, she shared her firm's new product development process, which was a process she had been involved in developing and benchmarking. Others who were also involved in developing the process later informed her that she shouldn't have shared it. It took extensive discussions with a significant number of people in the firm about the pros and cons of sharing the knowledge before a resolution was reached.

In another example, an industry executive at a large company reported that he attended a meeting with someone at another firm developing software. Upon his arrival, the developer gave a 90-minute presentation about his software. At the end of the meeting, the developer pulled out a non-disclosure agreement (NDA). The week before, the executive had received a lecture from his corporate counsel explaining why employees at the firm cannot spontaneously sign NDAs with other companies. The reason was that no one individual in the firm has the knowledge about what everyone else is working on to know that the firm hasn't already worked on that same issue and that this might be a conflict. Given the recency of this lecture, the executive refused to sign the developer's NDA, discovering later that someone in his firm was working on a similar concept. Thus, knowledge in emergent processes is distributed across many individuals making it difficult to ascertain in advance what is known to the organization and should be kept confidential.

When knowledge in emergent processes is distributed across individuals, the implication is that each person only has incomplete knowledge. It is only by piecing together each individual's part of the knowledge that a more complete picture of a situation can be appreciated. Thus, in an emergent process, any single individual's knowledge may be harmless or useless to individuals in other firms; when combined with other knowledge, however the pieced together knowledge may become far too useful to others, constituting a breach.

In sum, there are two processes that are emergent: cross-enterprise collaborative knowledge sharing, and the decision that leads to an information security breach. Therefore, pre-defined edicts about what can and cannot be shared are unlikely to be of value. Moreover, the success of the emergent collaborative effort is dependent on individuals being able to take advantage of collaborative opportunities. Simultaneously, individuals are confronted then with a series of opportunities to commit information security breaches opportunistically. In the next section we look at what individual factors influence how an individuals collaborates without committing these breaches.

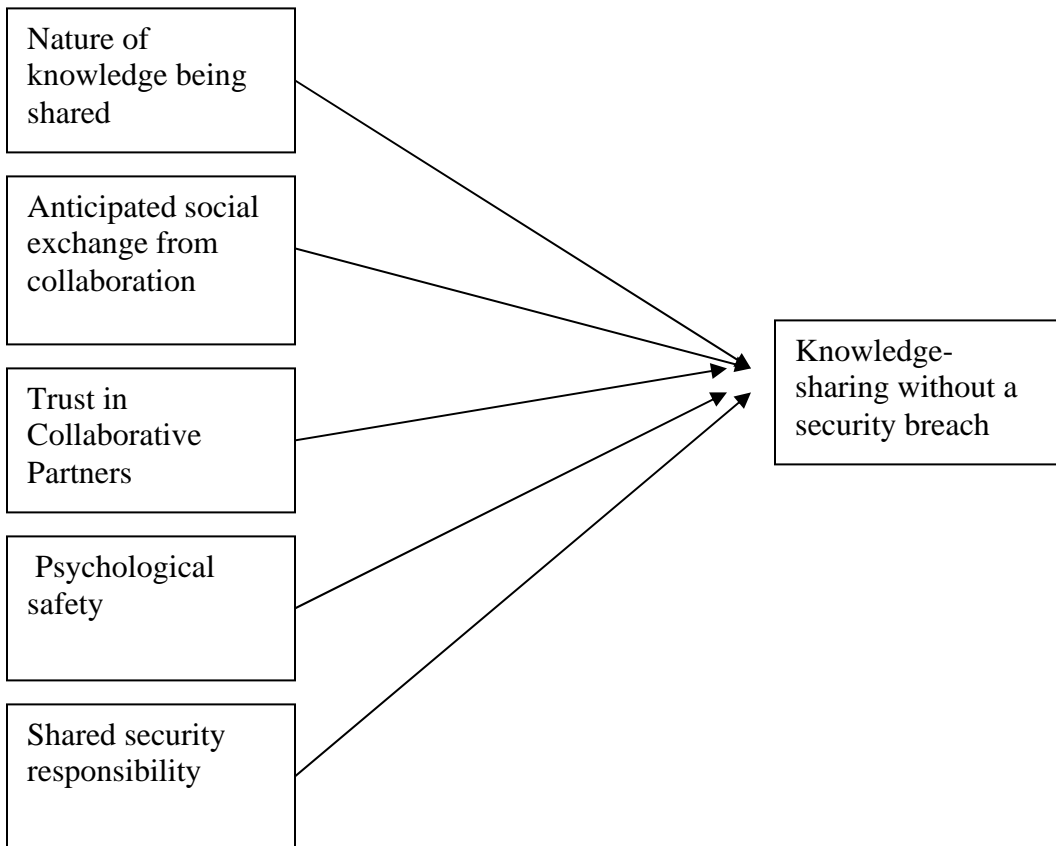
4.0 Individual-level Factors that Reduce the Probability of Information Security Breaches in Collaborative Knowledge Sharing

Consider a situation in which two individuals from two different organizations engaged in a discussion. What individual factors will keep these individuals productively

engaged in the conversation without sharing trade secrets, access, or information that could be used unfavorably as the conversation proceeds unpredictably? Theories drawn from social psychology, information systems, and organizational behavior and design would predict that five factors affect whether an individual will commit an information security breach. These five factors, depicted in Figure 2 are:

- 1) Nature of knowledge being shared
- 2) Anticipated social exchange from the collaboration
- 3) Trust in the collaborative partners
- 4) Perceptions of psychological safety with the firm and collaborative partners
- 5) Shared responsibility for security

Figure 2: Individual-level Factors Reducing Likelihood of Breaching



4.1 Nature of Knowledge Being Shared.

Given the situation-specific nature of the definition of what is secret, it is important to predict which types of knowledge under which conditions are more prone to unintentional security breaches. Drawing from two different sources suggests a framework for understanding when the nature of the knowledge being shared may be more or less prone to security breaches. The first source, from research by Jarvenpaa and Staples (2001), found that individuals engaged in collaborative knowledge sharing distinguish between sharing organizational products vs. personal expertise. They found that these distinctions had dramatic effects on how individuals share knowledge. Organizational products are viewed by employees as belonging to the organization and are therefore bound by the rules of the organization about sharing. Personal expertise, however, is considered part of their personal identity, and thus is not considered bound by the rules of the organization. This suggests, then, that the perception of who owns the knowledge is critical in determining if there is likely to be an information security breach. A firm may believe that knowledge has been shared that should not have been, and yet the employee may believe that the firm has no rights of ownership over that knowledge.

The second source is research by Hardy et al (2003). In their research, they found three reasons for collaborating: knowledge creation, resource sharing, and influence. In this research, it was found that the reason for collaborating determined how people collaborate and what knowledge they share. To obtain the benefits of the first reason -

resource sharing - required that both parties to the collaboration engage in intense back-and-forth conversations. To obtain benefits of the second reason – influence -- knowledge often needed to be shared primarily not between the two partners but with third parties (e.g., managers, vendors, funders). Finally, to obtain the third reason - benefits of knowledge creation – knowledge was shared both with third parties as well as in intense back-and-forth conversations with each other.

In Table 4, we have juxtaposed the findings from these two research studies. What we find from an examination of this table is the hypothesis that when individuals are engaged in collaborative activities for the purposes of knowledge creation, and are sharing what they consider to be their personal expertise, the risk of information security breach is the highest. This risk is highest because people engaged in intense conversations are likely to unwittingly share information they shouldn't; moreover, the inclusion of third parties increases the possibility that someone who shouldn't be trusted with the information will gain access to it. Finally, the fact that personal expertise is being shared suggests that individuals may fail to consider that the knowledge is organizational property, especially if the sharing yields new knowledge and greater personal expertise.

One industry executive described an example in which collaborators within a firm would informally discuss a product over lunch in the firm's cafeteria. A third party who was given access to the premises because of his collaboration with the company on a different product would informally join in the conversations. Unbeknownst to the

collaborators, the third party was using the knowledge gained from those conversations to leap ahead of the development team. After about eighteen months, the third party essentially “black-mailed” the company into a joint licensing agreement for the product.

Table 4: Hypotheses about Risk Potential of Information Security Breach for Different Types of Knowledge Content Shared

Purpose of Collaboration	Who Owns the Knowledge?		Likelihood of breach
	Organization	Individual	
Shared Resources	Lowest risk	Moderate	Low
Influence	Low	High	Moderate
Knowledge creation	Moderate	Highest risk	High
Likelihood of Breach	Lower	Higher	

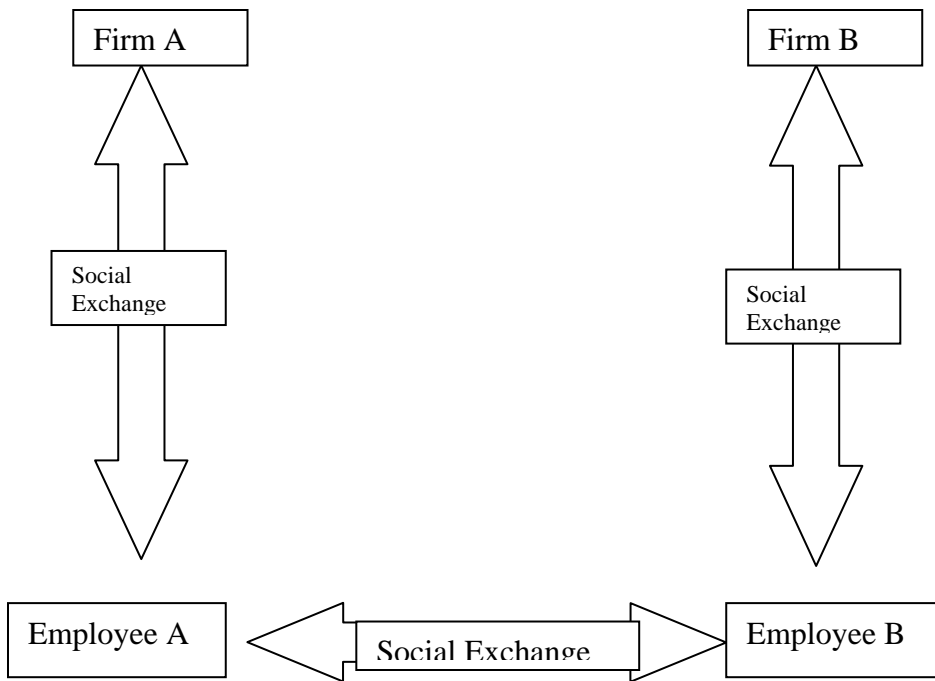
4.2 Anticipated Social Exchange.

In emergent processes, costs and benefits are situation specific, based on the dynamics of the collaboration. How a participant assesses these dynamic costs and benefits can be predicted by Social Exchange Theories (Blau, 1964; Ekeh, 1974). Social exchange theories argue that members of any relationship obtain social resources from that relationship, and that such a relationship extends to the workplace (Cole et al, 2002). These social resources include affiliation, social acceptance, and social support. As depicted simply in Figure 3, in any collaborative effort, there are three social exchanges that are occurring simultaneously in any cross-company collaboration: a) between Employee A and her organization, b) between Employee B and his organization, and c)

between Employee A and Employee B. The theory of social exchange was extended by Kelley and Thibaut (1978) to suggest that, in any relationship, when the amount of social resources accruing to any individual in that relationship fall below a comparison level of an alternative, the person will shift their social resources into the alternative relationship. This suggests, then, that employees engaged in collaborative relationships will give and receive more social resources from their collaborative relationships when they feel that the relationships they have with their organization are not providing those resources.

The notion that a disgruntled employee is more likely to commit security breaches is encompassed in Social Exchange Theory. However, the theory goes beyond simply looking for the obvious signs that lead to disgruntlement (e.g., low performance ratings, being passed over for promotion) and obvious symptoms (e.g., repeated expressions of dissatisfaction with the firm, job or supervisor). Instead, social exchange theory suggests that even satisfied employees may be at an increased risk of committing a security breach when the social resources they obtain from their employer is less than the resources they obtain from their collaborator. Waiting for outward signs of a lack of affiliation may be too late.

Figure 3:
Depiction of Social Exchanges in a Collaborative Relationship



4.3. Trust in the Collaborative Relationship and Firm.

In any collaborative relationship, there is information asymmetry (i.e., where one party knows more than the other party) about different aspects of the knowledge being discussed. In such situations, trust is critical since, it is very easy for a dishonest party to masquerade as an honest one, especially on the Internet (Ba & Pavlou, 2002). The amount of trust in the collaborative relationship will therefore dictate how knowledge is shared and access offered. The literature on trust between parties in internet-based commerce has concluded that one party trusts the other when Employee at Firm A feels that Employee B at Firm B is *benevolent* (i.e., acts in a way that represents “goodwill” toward A) and when Employee B is *credible* (i.e., repeatedly acts trustworthy by meeting commitments, etc) (Currall & Judge, 1995; Keen et al, 2000; McAllister, 1995; McKnight, et al, 2002; Sheppard & Sherman, 1998). To develop this trust requires Employee A to: a) have some familiarity and prior interaction with B to observe B’s actions in a variety to settings, b) be able to calculate the costs and benefits of Employee B cheating, and c) have knowledge of Employee B’s institutional structures supporting acting in a trustworthy fashion. In an emergent process, familiarity and knowledge of Employee B’s firm is likely to be distributed throughout the organization. That is, it may not be the case that Employee A at Firm A knows these things about Employee B at Firm B, but presumes that someone at Firm A knows these things. Thus, the Employee at Firm A may inadvertently give access to Employee B at Firm B with a higher level of trust than that which Employee B deserves. This suggests that the level of trust an individual

has in the other party will influence breaches. If an individual feels a high degree of trust, he may share more access than he should. Moreover, the distributed nature of the information about partners may lead to a false sense of trust with the collaborator.

While trust in the collaborator may increase the risk of a security breach, this risk can be counter-balanced by individuals' desire not to betray the trust their organization has in them. Research on betrayal has identified several factors that affect an individual's cognitive decision to betray a party's trust (Elangovan & Shapiro, 1998). These include: benefits of betrayal outweighing penalties, presence of a relationship with the trustor that has become unsatisfactory, and seriousness and clarity of ethical principles involved. No one factor alone has been found to be sufficient to explain betrayal: *all are needed*. The current information security literature has focused on the first: if more benefits were allocated to information security protectors and greater penalties allocated, then possibly there would be fewer violators. However, all three factors taken together have not been part of a comprehensive information security policy.

Moreover, in an emergent process, it may be difficult for the individual to determine the seriousness and clarity of ethical principles involved. An individual who fails to turn off their computer at the end of the day because they plan to login to her desktop the next day remotely – does that person believe she is violating an ethical principle, or in fact is being very efficient? That is, the individual may believe she should be rewarded for her focus on productivity, not accused of ethical violations. Moreover, without providing the individual with information about the seriousness of the risk

incurred by her behavior, her decisions are likely to favor that which she knows the most about: her own productivity.

Failing to keep employees informed of the seriousness of committing a security breach is a common practice in firms today. An industry executive reported an example of such a case. In this case, the customer for a project sat down with project managers to define what information was considered so sensitive that it shouldn't be shared between the firm and its collaborating suppliers. Instead of training the several hundred engineers doing the work on what information should not be shared and why, the firm decided that such training was cost-prohibitive and employees could not be trusted to make the right judgments anyway. So the firm hired and trained six "information protection" officers in these ethical principles. However, without the training, the hundreds of engineers proceeded with their work without a clear specification and appreciation for the importance of the ethical principles involved in sharing their work with others. Moreover, without the training, the engineers were deprived of any opportunity to provide feedback to the customer about the ethical principles specified (were they too broad? Did they help to distinguish unethical behavior? Did they harm work performance?). Finally, the instructions from the customer did not distinguish between more critical ethical breaches and less critical ones, which made it more difficult for the employees to make value statements when they were in the "grey zone".

Criticality of breaches is an important consideration in any employee's internal calculus of the cost of the breach. Breaches that have a greater negative impact to the

firm require much greater benefits before the employee is willing to commit the breach. . It may be possible to classify criticality – not just based on a corporation’s competitive position in the marketplace, but more generally. Using Perrow’s (1999) notions of complexity of interactions and tightness of coupling between subsystems, one could argue that breaches in which the knowledge shared has more complex interactions and tighter coupling with other knowledge are much more serious breaches than breaches that can be “self-contained”.

For example, in one anecdote provided by a security firm, the firm reported that most of its customers had no knowledge that when they visited websites, the cookies that were automatically downloaded made them vulnerable to attack. They were also not aware of the “social engineering” attacks propagated by hackers (in which people share information with hackers without even knowing it). Moreover, they were not aware that as individual home computer users, they were likely to be propagating viruses. Finally, they did not know that they were inadvertently sending unencrypted email. Without the information about the impact of their actions, individuals do not see themselves as violating a trust.

4.4. Psychological Safety in Firm and Collaborative Relationship

An emergent process is above all else a learning process. To facilitate a learning process requires such learning behaviors as seeking feedback, sharing information, asking for help, talking about errors, and experimenting (Argyris, 1993; Edmondson, 1999).

Individuals feel psychologically safe when they believe they can engage in these learning behaviors without being rejected. In a study of hospital patient-care teams, significant differences in members' beliefs about social consequences of reporting medication errors were observed (Edmondson, 1996). When they don't feel "safe", individuals will act in ways that inhibit learning, including failing to disclose errors and not asking for help.

In the information security context, two sets of learning processes are occurring simultaneously: a) learning that occurs between the collaborators, and b) learning that occurs among individuals in the firm about how to collaborate securely. Theoretically, an individual should commit fewer breaches when they feel psychologically safe with both processes. In the collaborative process, psychological safety should allow the individual to admit mistakes with the collaboration if access or information is inappropriately shared, and seek help in rectifying the mistake, such as by asking for the return of confidential documents and obtaining assurances that they were not copied. Similarly, psychological safety with the organization should allow the individual to admit mistakes (e.g., breaches) to her supervisor or IT Security Administrator and not be rejected. The interesting case is when the individual feels little psychological safety with her organization, and significant psychological safety with the collaborator. Such a situation may be at the highest risk for security breach since the individual will be unable to learn from her organization to identify ways to avoid future breaches.

4.5. Shared Responsibility for Security

Viewing information security from an auditing perspective, a mechanism for avoiding security breaches is to ensure that no single individual is responsible for performing conflicting duties within or between processes (Rasmussen, 2004). Example conflicting duties include employees who have the authority both to add a vendor and to pay an invoice to that vendor, authority to both create customer invoices and enter payments from customers, and the authority to both create an employee and change that employee's salary information in the database. Differentiating conflicting duties leads to having one person responsible for one action and another responsible for the other action. This orientation is at the heart of many organizational structures designed to reduce security breaches. For example, allocating responsibility for creating and enforcing information security strictly to a project manager or to corporate lawyers or to information security professionals are examples of dividing duties for security away from the employees performing the core work.

While this approach of differentiating responsibilities for security may succeed at removing the possibility of conflicts in routine work, it doesn't work for the emergent process of collaborative knowledge sharing. In emergent work, knowledge sharers are constantly confronted with the possibility of conflicts: of recommending vendors at the same time as suggesting how they should get paid, of sharing knowledge about third parties, of sharing technical knowledge before they even know if an idea is patentable. Moreover, roles and interest in security emerge unpredictably as the need arises. In one firm, a contract manager became quite adept at preparing contracts with business partners that pre-empted legal concerns about information disclosure – essentially collapsing the

legal and contractual issues into one efficiently performed role. In another firm, a team agreed to accept full responsibility for their own security monitoring instead of having professional security personnel monitor them. The team appointed and rotated monitors and discussed security risks at frequent meetings. In a follow-on evaluation, this team was found to have committed fewer security violations than a team monitored in the traditional way by information security professionals. Thus, by giving individuals authority to exercise judgment about security decisions, combined with the close monitoring by peers, the team was successfully able to avoid security breaches.

5.0 Implications for Organizational-Level Facilitators for Promoting Security in Knowledge-Sharing

The individual level factors in the previous section suggest several organizational-level facilitators of information security behavior. In this section, these organizational-level facilitators are described.

5.1 Include Social Resources in Psychological Contracts Between Employee and Firm

If collaborative knowledge-sharing without a security breach is more likely when the employee receives greater social resources from their organization than from the collaborative relationship, results from research on how to strengthen social exchanges inside a firm guide us in identifying organizational facilitators to reduce the possibility of

security breaches. Research on what are known as “psychological contracts” may provide some guidance (Lambert, et al, 2003; Rousseau, 1995). Psychological contracts are the set of obligations expected of the employee compared to the obligations (also called inducements) offered by the firm to the employee. When entering into any relationship, psychological contracts are negotiated (albeit implicitly for everything but pay). As the employee begins to deliver on her obligations, and the firm delivers on its obligations, the employee makes an ongoing assessment of whether the psychological contract has been upheld.

Research has repeatedly demonstrated a correlation between employee attrition and the presence of a perceived breach in the psychological contract. If employees must receive social resources from the firm, then the psychological contract must include social resources, such as recognition, development, feelings of self-worth, and affiliation. However, research on psychological contracts also indicates that employees must see the firm’s inducements as “commensurate” with their view of their own work; over- and under-inducements are equally problematic. Thus, if the employee feels she is barely fulfilling her obligations to the organization and yet receives an abundance of social support, she will be equally likely to leave (or behave in a way that violates corporate policies) than an employee that feels she gave everything to the organization and received nothing in return. This suggests, from an organizational perspective, that social resources such as recognition, development, self-worth and affiliation need to be explicitly negotiated and renegotiated during an employee’s tenure at the firm if the risk of security breaches is to be minimized.

5.2. Encourage Sharing About Security Risks

If employees may develop false impressions of trust in collaborators because knowledge about the collaborator is distributed within the firm, knowledge about past collaborations should be shared. Some firms have argued that “impressions” about others should not become “public” knowledge and therefore should not become distributed electronically in a distributed organization. However, careful planning to decide what type of information about past collaborations should be shared can overcome this concern over sharing unstructured, ill-informed impressions.

One suggestion made by an industry executive about the type of information to share regarding past collaboration that might be useful was to have employees simply share short stories about past collaborations that describe what happened when a technical (not security related) issue could not be resolved by those directly involved in the collaboration and was elevated to higher-level managers. Such stories might provide information about whether partner firms (or individuals at the firms) acted benevolently and met commitments. Another suggestion (Perrow, 1999) is to have a firm review its previous collaborations to identify early warning signals for the problem collaborators. One such signal might be the speed with which the collaboration evolved, with more quickly induced collaborations leading to less due diligence in learning about the other party. Another signal might be the collaborator’s response to unexpected events: has the partner been flexible and learning-oriented? Past experiences with the collaborator in

sharing errors might also be an early-warning signal: failure to share errors may later lead to failed collaborations. Finally, since collaborators who act as lone cowboys in a marketplace may not be part of a rich network of organizations, regulators, and constituencies that monitor and intervene in cases of breaches, the density of a collaborator's network may provide an early warning signal.

Regardless of the precise nature of the information shared about past collaborations, the individual factor of psychological safety requires that employees must be convinced that they can share this information within a "safe haven", without fear of retribution. Otherwise, the employees will withhold the knowledge, increasing the possibility that other employees will develop false trust in partners, and not learn from mistakes made by others to enhance security.

The distributed nature of security-related knowledge also suggests that efforts to share security-related knowledge across organizations are needed. One executive reported that something like a "Security Net" is needed in which alerts go out that trigger people across academic, government, and private organizations to help resolve – "a virtual swarm of good guys". Incentives to support this knowledge-sharing effort would be needed.

5.3. Security Technologies and Policies Integrated into the Work Process.

Significant literature on technology ease-of-use indicates that employees will not use technologies (broadly defined to include procedures as well as software and hardware) as intended to improve performance if it requires them to change their behavior in ways they believe do not support the purpose of their work (referred to as the task-technology fit). Unfortunately, information security policies and technologies have been designed as “add-ons” to an employee’s normal workday. For example, to require users to remember to turn off their computers at the end of the workday creates an additional cognitive load, as does the requirement to change one’s password frequently using a combination of different symbols (all of which are difficult to remember, thus resulting in little post-it notes with the password written on them – notes easily copied by others). Moreover, to expect home users to download cookie-banning software, purchase virus protection software, and frequently download software updates to patch bugs puts a substantial cognitive burden on the individual (both because of the stress involved when the downloads fail to work, and the requirement to remember to do the downloads). Instead, systems need to be designed to reduce cognitive load on the worker – to make security a part of one’s work. For example, having computers monitor a safe to automatically lock it when someone leaves the room is much more likely to lead to secure behavior. Similarly, computers that automatically lockdown the computer when it is left unused for a short period of time, requiring the user to reenter a password upon return might be a minor nuisance, but is only less imposing than alternatives.

The emergent nature of collaboration also suggests that the tools and procedures must be “self-deploying” and “seductive”, meaning that they must draw people into

‘doing the right thing’, sometimes without them realizing it. Seductive, self-deploying procedures are ones that are unobtrusive yet intentionally designed to serve the individual as a customer (not as a potential risk or perpetrator). Examples of unobtrusive, customer-oriented policies and tools include intelligent agents which detect patterns in behaviors and suggest to the collaborator some alternative course of action, or the use of “collaborative filtering” systems that help individuals understand how documents have been used in the past in creative ways to protect trade secrets, or the use of automatic routing systems that inform managers not only of the need to make quick decisions to release a document but information to facilitate the decision-making. The point is to provide support and guidance to the individual engaged in the collaborative effort, not onerous procedures.

In addition, security policies that are integrated into one’s work help people make the emergent decisions they are confronted with on a daily basis. Simply prohibiting the release of information is unhelpful since any collaboration requires release of some information. Moreover, requiring employees to turn to project managers or security personnel has two negative side effects: a) it places additional time and effort burden on the employee and b) it removes any sense of responsibility from the employee over actions taken. Instead, security policies should help the employee understand types of security-related decisions that they are making on a regular basis, criteria and factors to consider in making these decisions, and leadership roles they can play in helping others make these decisions. Possible roles include “opportunity recognizers” who help to recognize when a high-risk situation may occur, “chauffeurs” who help people learn and

apply information security policies, and “stewards” who facilitate workers to capture practices that lead to better decision making about the tradeoffs between sharing and not sharing knowledge. This suggests that managers need to closely watch their employees to identify individuals that have a propensity to understand security implications of conversations and actions. Providing both peer and managerial recognition of this propensity, as well as recognizing its important value to the technical competence of an employee is critical. For example, helping engineers to understand how to collaborate with other companies in ways that protect corporate interests is a skill and talent that should be rewarded as part of technical competence building.

The emergent nature of collaborative knowledge sharing also suggests that people behave based on feedback not based on standard procedures. Thus, they need dynamic detailed feedback on their work that encourages them to behave securely. If others are accessing employees’ documents, employees should be informed about who is doing the access so they can become part of the security process of determining what might be suspicious access. If employees’ passwords are being used from different desktops than previously used, employees should be notified so they can take action. If employees are considering sharing certain knowledge with outside collaborators, employees should be able to query their portals to see if previous similar knowledge sharing has occurred.

5.4. Develop Policies That Align Individual, Group, & Organizational Concerns

When collaborating, information security designers must recognize that individuals are representing at least three organizational levels in the cross-organizational collaboration: themselves as individuals, the group (project team, department), and their organization. As depicted in Table 5, the issues are different at each of the three levels. At the individual level, the concern is about protecting personal privacy (Chellappa, 2004; Culnan, 2000; Culnan & Armstrong, 1999), mobility, and expertise. At the group level, the concern is with protecting under-developed group ideas, avoiding inefficient use of the time (such as is spent when unshared knowledge needs to be reinvented), and developing a strong group identity. Finally, at the organizational level, the concern is with protecting intellectual property, liability, and reputation. At each level, there are tensions between protection and sharing. At the individual level, individuals want to protect their expertise since that is what they are recognized for, but they also want to develop that expertise further during the collaboration effort. At the group level, there is a tension between protecting under-developed ideas and the innovation that comes from sharing those ideas with outsiders. At the firm level, reputation and intellectual property are enhanced through sharing, not through protection.

An individual engaged in a collaborative effort is attempting to balance these tensions at all three levels. Recognizing that the levels may present conflicts and identifying similarities across the levels may help employees in making decisions that optimize one over the other at appropriate points in time. Additionally, it may be possible to identify perspectives that help to resolve the tensions across the levels and between protection and sharing. For example, expertise development and protection is an

issue consistent across the levels. If a consistent policy could be developed that articulates expertise needing development vs expertise needing protection for the firm, then this may help to resolve the tension across levels by helping employees and groups focus their sharing efforts on that expertise to develop. As another example, establishing certification programs that organizations interested in collaborating with others must obtain would allow collaborating individuals to more safely assume that collaborators have necessary protections in place, creating less conflict between levels.

Table 5: Tensions Across Levels

Level	What to Protect During Collaboration	What to Develop Through Collaboration
Individual	Privacy; expertise; mobility	Expertise
Group	Expertise; under-developed ideas; time; identity	Innovation, expertise, group access to external knowledge
Firm	Protection of IP, liability, copyright, reputation	IP, reputation, copyright & risk-sharing

5.5. Provide Tools to Help Employees Dynamically Weigh Costs & Benefits of Acting Securely

Because collaborative actors are sharing knowledge opportunistically, the costs of sharing a piece of knowledge (i.e., potentially creating an information security breach) against the benefit of sharing the knowledge (for increased collaboration and possibly obtaining secret knowledge from the other firm) are dynamic. Moreover, because these individuals are often concerned about efficiently using their time, they are also dynamically judging the trade-offs between strictly following security procedures against the efficient-costs incurred. Policies alone are insufficient. Employees can benefit from tools that support them in making these decisions dynamically.

Some of these tools are management actions. These managerial tools include continuous discussions among employees about what are the “corporate jewels” of the organization. For example, in one collaborative effort (Majchrzak et al, 2000), a manufacturing engineer at one company engaged in a ten-month design effort with rocket engineers at a second company. The engineer at the first company understood that his division’s corporate jewels included the analytic tool he and others had developed to assess the manufacturability of a part. Therefore, the engineer understood that it would be inappropriate to share the code or the specifics underlying that analytic tool. However, the engineer also understood that his real value to the partner company wasn’t the analytic tool. Rather, the value came from the judgments he made based on his use of the analytic tool about the manufacturability of a proposed part during intense brainstorming sessions. In this way, the engineer was able to respond quickly as various

configurations of parts were proposed, enabling the team to more quickly converge on a manufacturable solution.

Tools to help in this tradeoff are not only management actions, but also can be technology-based. Algorithms for intelligent agents containing keywords based on corporate jewels can be developed to peruse documents under development as well as email traffic to notify employees when they might want to discuss the sensitive nature of their work with others. Peltier (2001) offers a set of nine factors, listed in Table 6, which should be included in this algorithm to calculate the value of the information asset. By having intelligent agents provide meta-tags describing the likely value of a document to others outside the firm, employees and managers can begin to refine the agents' algorithms. Moreover, if these comments about value could suggest consequences of allowing other firms to see this knowledge, the employee would be better able to assess the relative value of sharing vs the value of keeping it within the corporate walls. Tools such as these help employees to engage in the sharing process fully supported and informed to maintain and evolve a company's corporate jewels, not as ignorant violators. Walls et al (1992) have referred to such tools as vigilant information systems.

Table 6: Peltier's (2001) Factors Upon Which Value of an Information Asset Should be Based

- Cost of producing the information,
- Value of the information on the open market,
- Cost of reproducing the information if destroyed,
- Benefit the information brings to the enterprise in meeting its business objectives or mission,
- Repercussion to the enterprise if the information was not readily available,
- Advantage it would give to a competitor if they could use, change, or destroy the information,

Finally, technical tools can be developed that not only provide employees information about the impact of their knowledge-sharing behavior, but also about the impact of their computer usage on the probability of security breaches. Given that existing theory suggests that employees are more likely to follow security procedures if they understood the implications of not following them, tools that help to remind employees of the impact of not following security procedures may be useful. One example might be to provide employees, free-of-charge, with a small security-oriented icon (or dashboard) in the corner of their screen. When used within a corporation, the icon might indicate the number of attacks on the corporate network, and the number of accesses attempted on their hard drive over the last hour. When the icon is on a home computer, it might indicate the number of cookies on the hard drive, the number of times since login that unannounced others have used the computer, and the number of times certain files had been accessed. With click-throughs, suggestions could be offered on how to reduce the numbers, with the numbers updated often enough for the user to visibly observe the impact of their behavior.

5.6. Matching a Firm's Information Security Strategy with the Market.

There are two aspects of information security strategy. One aspect directly affects the trust and psychological safety of the employee. This aspect concerns the attributions that executives make when security is breached. Does the executive management take a denial-oriented approach to security breaches, such as First Energy did with the August

14th 2003 energy blackout in Northeast U.S. and Canada? Are there cover-ups with people unwilling to accept any responsibility? In contrast, is there an openness to sharing knowledge about possible factors that may have increased the probability of a breach to determine how to avoid it in the future? Then, how is this strategy implemented internally in the organization? Are employees who write memos warning of the possibility of breaches or errors ignored or, worse chastised? When security breaches occur, is more emphasis given to finding someone to blame than to truly understand the problem systemically to avoid it in the future? Or are such concerns dealt with in an open and thoughtful manner?

A second aspect of information security strategy is the posture in the marketplace that the firm takes to information security. Cramer (1999) argues that firms take one of five approaches to preventing information breaches: 1) *defensive* (involving significant access controls and reduced interconnections), 2) *offensive* (involving denying information to competitors), 3) *quantity* (involving making attaches impractical because of the sheer volume and timeliness of data releases), 4) *quality* (in which information is protected through better information management, and 5) *sponge* (in which information is protected through better information collection about possible breaches). Although Cramer does not suggest that one strategy is better than another, it could be easily postulated that a strategy is best when it is matched to the market context, the firm's corporate position in that market, and the firm's internal culture of knowledge-sharing. A firm that is the market leader through innovation may be a more successful collaborator when it adopts an information security strategy that is based on quantity or quality, while

a firm adopting an approach to the market based on operational excellence may be more successful when its information security strategy is either sponge-like or defensive.

Individuals working in a firm with a matched security strategy would be hypothesized to be less at risk of a security breach because directions about how the company handles security threats are clearer. Thus, having a matched strategy is likely to be a facilitator.

6.0 Summary of Organizational-level Facilitators

Table 7 presents a summary of these organizational-level facilitators, juxtaposed against the characteristics of an emergent process. Apparent from the table is that the emergent nature of both the collaborative knowledge-sharing process and the decision to commit a security breach create the need for a different set of security interventions than ones used in the past.

Table 7. Organizational Facilitators for Emergent Nature of Securely Sharing Knowledge Collaboratively Across Firms

Characteristics of Generic Emergent Knowledge Processes	Characteristics of Information Security Decision-making within CKS	Generic Principles for Facilitating Emergent Knowledge Processes	Organizational Facilitators for Secure Knowledge-Sharing
Problem deliberations, interpretations, and actions unfold unpredictably	Sharing of secret knowledge is a matter of interpretation; costs vs. benefits are situation specific and judgmental based on dynamics of collaborative knowledge-sharing	Provide information on tradeoffs, relationships between variables and consequences of alternative decisions based on expert judgment and data	<ul style="list-style-type: none"> • Provide tools to keep employees dynamically informed of the probable consequences of their actions; • Provide feedback to employees on metrics throughout work process that encourage secure behavior
Unpredictable user types, process leaders, and work contexts	New internet technologies always emerging; Triggers for information security decisions unpredictable; Autonomous decision-making with imperfect oversight	Use of specific tools and procedures must be self-deploying and “seductive”; allow leaders to emerge	<ul style="list-style-type: none"> • Ensure security procedures and tools are integrated into work processes and “seductive”; • Develop policies that align Individual, Group, and Organizational concerns; • Include social resources into firm-employee psychological contracts
Difficult-to-share tacit knowledge is distributed across people and places	Information about what is secret, why, implications of sharing with external parties, which external parties are trustworthy collaborators, and which internal agents are high-risk is distributed and often tacit	Provide forums for sharing knowledge; provide qualitative performance metrics of work processes with definitions that encourages involvement and attention for all parties	<ul style="list-style-type: none"> • Encourage within-firm sharing about past collaborations that are “safe havens” • Encourage cross-org sharing about info that may identify risks • Match firm’s information security strategy with market

7.0 Implications for Research

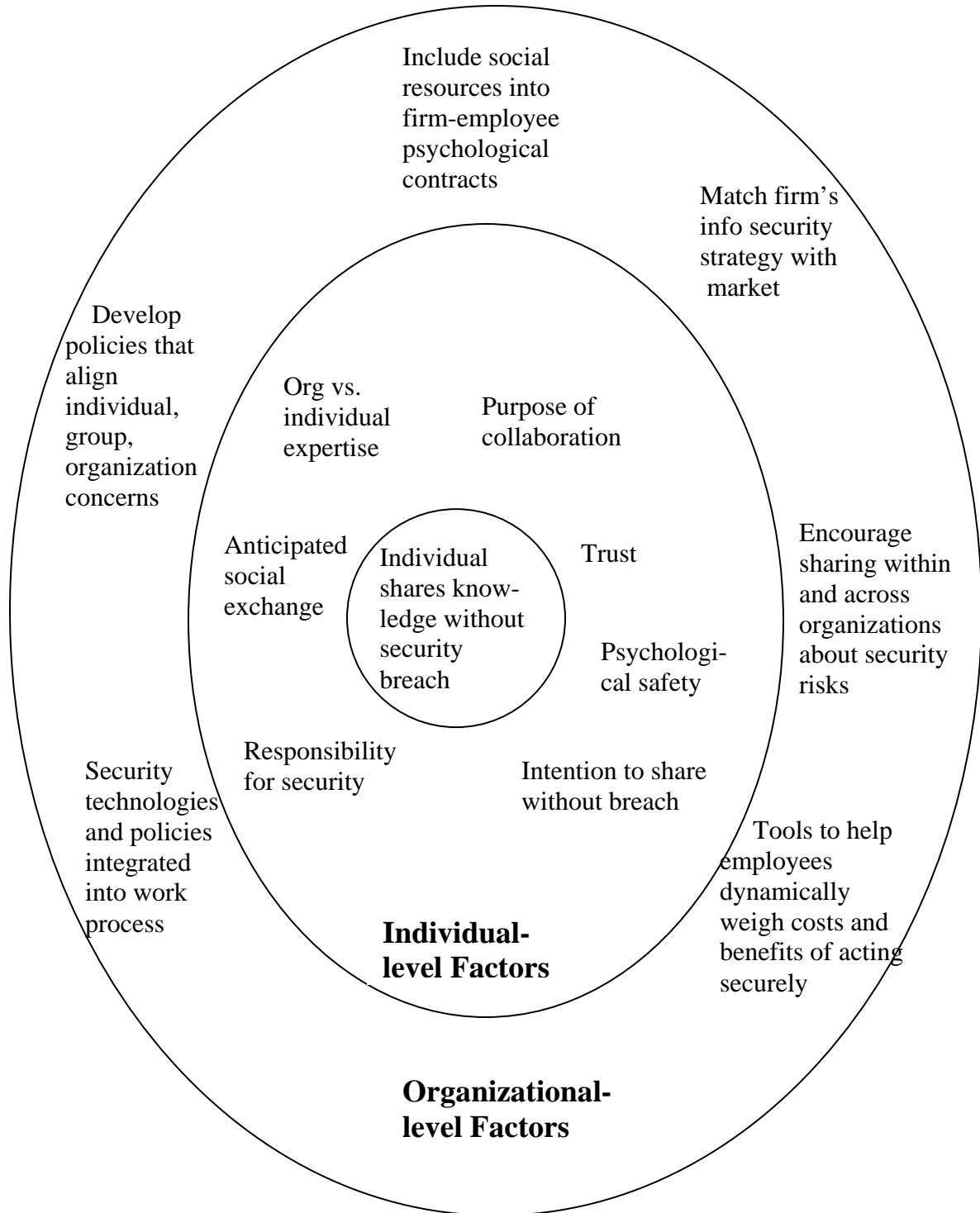
Figure 4 depicts the complete framework. Given the importance of this topic and the untested nature of this framework, research is needed to immediately test the framework.

Such a research program should have five components:

1. Conduct case studies and surveys of industry and government practice comparing cases of collaborative knowledge sharing with and without information security breaches. Such research can be used to validate and elaborate the conceptual framework.
2. Conduct “Misinformation” experiments in which misinformation is purposely made available to selected organizations and individuals which vary on the dimensions of the conceptual framework to provide further validation and elaboration of the framework. This is a technique often used in counter-intelligence operations and cyber terrorists but rarely applied to the study of cross-organizational collaboration.
3. Conduct action research and pilot studies with existing software packages that monitor email traffic (e.g., AskMe, Tacit) and work processes to determine their value for providing employees with the information needed to make dynamic cost/benefit tradeoffs
4. Engage in technology development of intelligent agents embedded in email systems and documents to provide collaborators with help in deciding dynamically what should and should not be shared.
5. Undertake the pilot development, deployment, and evaluation of two types of highly secure cross-organizational networks: a) one for sharing security-related information to quickly react and predict breaches and b) one for

organizations wanting to start a collaborative effort to quickly open technical discussion forums that are certified to be secure.

Figure 4. Conceptual Framework of Critical Success Factors to Support Individuals Sharing Collaborative Knowledge Without Security Breaches



Such a five-pronged approach to research would help to answer a range of questions that a focus on the individual simultaneously engaged in the emergent processes of collaborative knowledge sharing and protection of information security raises. Example questions are offered in Table 8. These questions need to be resolved to identify interventions that most effectively and efficiently reduce information security breaches in cross-organizational collaboration.

Table 8: Sample Research Questions Needing to Be Answered To Identify Effective and Efficient Security-Protection Interventions in Cross-Organizational Collaborations

- 1) When an employee shares knowledge collaboratively with an outside organization, what factors influence what knowledge is considered appropriate to share from an information security perspective?
- 2) Some analysts argue that the problem with security breaches is just lack of information and awareness that one's own behavior is part of a network that allows hacking and breaching. Is this true? If people had the knowledge only, would they act on it, or is the situation more complex, as suggested by the conceptual framework offered here?
- 3) One person interviewed for this report (a vice-president of homeland security for a large corporation) argued that well-run large companies do not experience security breach problems when their employees collaborate. Is this true? Is this a problem exclusively observed among small and medium-sized companies?
- 4) Can the process of sharing knowledge collaboratively with outside firms be depicted in a general enough way to be applied across companies and in a specific enough way to be used to identify ways to measure the process? Can measures that differentiate between actions that are likely to lead to information security breaches be identified, and then unobtrusively measured? When these measures are compared to "overzealous" security policies, do the measures (and actions taken when the measures are monitored for suspicious behavior) yield better identification of possible offenders?
- 5) As argued in this conceptual framework, to encourage informationally-secure knowledge-sharing requires a different set of policies, tools, and job responsibilities than is currently used today. How do organizations gain practice on these new policies, tools and job responsibilities? One industry executive argued that corporate involvement in consortia are critical for gaining these skills since they cause individuals and the organization to adjust their old practices to accommodate collaboration. For example, in the executive's previous firm, there was enough collaborative activity to have developed the skills in a contracts officer to deal with 90% of the contractual issues involved in collaborations without going to the corporate attorneys and there were enough collaborative incidents such that the corporate attorneys gained confidence in the contract officer's ability to handle the issues well. Building this type of asset in the firm requires repeated collaborative partnerships. In a sense, collaboration breeds secure collaboration. This is a hypothesis quite worthy of study.
- 6) Why do employees ignore information security suggestions? Are the reasons similar to those suggested in this framework?
- 7) While energy in a collaborative knowledge-sharing activity is a positive thing for the organization, it should not be done at the expense of a relationship with the home organization. Where is the right balance?
- 8) Is it possible to develop a "vigilant information system" that collaboratively monitors the sharing of documents and knowledge to provide proactive feedback to users who are potentially violating information security policies?

(continued)

Table 8: Sample Research Questions Needing to Be Answered To Identify Effective and Efficient Security-Protection Interventions in Cross-Organizational Collaborations (cont)

- 9) Since trust in a collaborative knowledge sharing relationship is distributed throughout the organization, are the current notions of trust, which have been based almost exclusively on individual-to-individual behavior, appropriate? Does trust transfer across people, that is, if a collaborator is trusted by an employee, will another employee simply adopt that trust stance toward the collaborator? How do the two compare notes if their experiences are different – given that they may not even know that each is having a collaborative relationship? While third-party business-to-consumer trust mechanisms have been in place for sometime (e.g., Etrust), the penetration of business-to-business third-party trust mechanisms (e.g., webtrust.org, bbonline.com) is low. Can a third-party mechanism as used in business-to-business contexts work for collaborative knowledge sharing?
- 10) Can intelligent agents be developed that can scan documents for their tightness of coupling and complex interactivity with other documents, and then use this information to suggest a rating of the risk to the organization if the document was shared?
- 11) Several types of specific experiences from previous collaborations that could be shared among individuals in a firm considering collaborating with others were mentioned. When this information is in fact shared within or between organizations, does that organization have more success at collaborative activities that add value without security breaches?
- 12) Certification programs for security are not being used today as the basis for identifying and selecting collaborators, as well as the basis for setting up secure cross-enterprise forums for sharing technical knowledge or security knowledge. Why not? What are the political and social barriers, and how can they be overcome?
- 13) Technical aids to keep employees dynamically apprised of the consequences of sharing knowledge have been suggested. However, one industry executive called for need for research on whether appropriately trained security personnel who become informal members of high-risk project teams could also provide a similar service. Can either technical aids or security personnel provide a similar service?
- 14) Are there analogues in industry and government practice of people self-policing their collaborative interactions to avoid breaches that can inform us of how to structure similar self-policing for information security during collaborations? One possible analogue may be found in studying internet games. System administrators emerge in these seemingly “lawless” games such as CounterStrike, encouraging game players to act according to evolving norms through withdrawal of game privileges. Examining the characteristics of these emergent administrators, and the communities which foster their emergence, may provide additional suggestions on designing information security systems.
- 15) There are different types of collaborations: supply chain, new product development, outsourcing, non-profit, community-building, joint ventures, industry consortia, and electronic marketplaces. Does this framework apply equally to all types?
- 16) What is the optimal fit between a firm’s information security strategy and its market position?

8.0 Conclusion

Although this framework is largely untested, it offers some immediate actions that managers could implement now. These include:

- Integrate Information Security programs with Human Resource Programs.
- Identify people at risk of a breach, not based on obvious signals of disgruntlement, but based on those who are asking for little social resources from the firm.
- Instead of identifying required or prohibited behaviors when developing an information security policy, identify security-related decisions that each individual should make, leadership roles they can play in helping others make those decisions, and criteria and factors to consider in making those decisions.
- Expect that knowledge shared will depend on the employees' perceived purpose of the collaboration. Therefore, ensure that the employee's perceived purpose is the same as that of the organization.
- Develop mechanisms for sharing information within the organization about previous collaborations with a collaboration partner.
- Integrate security requirements into the work. Develop the technology so following these requirements is easy. Allow them to be personalized to the work.
- Develop vigilant information systems for the employees to use to make dynamic decisions about releasing information.
- More fully develop betrayal inhibitors by developing a close relationship between the employee and the firm; don't over-induce an employee.
- Don't create policies that assume that all information shared is of high value to the organization; instead provide ways for employees to assess how closely linked the information being shared is to corporate jewels.
- Work with employees to determine what is personal expertise and what are organizational products.
- Establish cross-organizational forums for sharing knowledge, alerts, and triggers to quickly respond to the distributed nature of breaches.

While organizations can take these steps immediately, the emergent nature of the collaborative process and the decision to commit a security breach leaves much that is still not well understood. This paper presents an attempt to provide a framework for further research.

9.0 References

- Argyris, C. 1993. *Knowledge for Action: A Guide to Overcoming Barriers to Organizational Change*. San Francisco: Jossey-Bass.
- Ba, S. and Pavlou, P. 2002. "Evidence of effect of trust building technology in electronic markets", *MIS Quarterly*, 26(3), 243-268.
- Blau, P.M. 1964 *Exchange and Power in Social Life*. NY: Wiley.
- Champlain, J. 2003. *Auditing Information Systems*, 2nd Edition. NY: Wiley.
- Chellappa, R. (2004) *Consumers' trust in ecommerce transactions: The role of perceived privacy and perceived security*. Los Angeles: University of Southern California Ebizlab.
- Cole, M.S., Schaninger, W.S. & Harris, S.G. 2002 "The workplace social exchange network: A multilevel conceptual examination" *Group and Organization Management*, 21(1), 142-167.
- Cramer, M. 1999. *Economic Espionage: An Information Warfare Perspective*, White Paper, Annapolis, MD: Windermere Information Technology Systems
- Culnan, M.J. 2000. "Protecting privacy online: Is self-regulation working?" *Journal of Public Policy and Marketing*, 19(1), 20-26.
- Culnan, M.J. & Armstrong, P.K. 1999 "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation" *Organization Science*, 10(1), 104-115.
- Currall, S.C. & Judge, T.A. 1995 "Measuring trust between organizational boundary role persons" *Organizational Behavior and Human Decision Processes*, 64(2), 151-170.
- Dervin, B & Shields, P. 1999. "Adding the missing user to policy discourse: Understanding U.S. user telephone privacy concerns" *Telecommunications Policy*. 23(5), 403+.

- Edmondson, A. 1996 "Learning from mistakes is easier said than done: Group and organizational influences on the detection and correction of human error" *Journal of Applied Behavioral Science*, 32, 5-32.
- Edmondson, A., 1999. "Psychological safety and learning behavior in work teams." *Administrative Science Quarterly*, 44, 350-383.
- Ekeh, P.P. 1974. *Social Exchange Theory: The Two Traditions*. Cambridge, MA: Harvard University Press.
- Elangovan, A.R. & Shapiro, D.L. 1998 Betrayal of trust in organizations. *Academy of Management Review*, 23(3), 547+
- Erickson, G.S., Rothberg, H.N. & Carr, C.A. 2003 "Knowledge-sharing in value chain networks: Certifying collaborators for effective protection processes" *Advances in Competitiveness Research*, 11(1), 152+
- Garg, A., Curtis, J. & Halper, H. 2003 "The financial impact of information technology security breaches: What do investors think?" *Information Systems Security*, March/April, pp22-33.
- Hardy, C., Phillips, N. & Lawrence, T.B. 2003. "Resources, knowledge and influence: The organizational effects of interorganizational collaboration" *Journal of Management Studies*, 40(2), 321-347
- Jarvenpaa, S.L. 2001 *Copyright and Business Patents in Software*. Report for the Society for Information Management Advanced Practices Council, Chicago.
- Jarvenpaa, S.L. & Staples, D.S. 2001. Exploring perceptions of organizational ownership of information and expertise. *Journal of Management Information Systems*, 18(1), 151+
- Keen, P., Balance, C., Chan, S. & Schrupp, S. 2000 *Electronic Commerce Relationships: Trust by Design*. Englewood Cliffs: Prentice Hall.
- Kelley, H.H. and Thibaut, J.W. *Interpersonal Relationships*, NY: Wiley, 1978.
- Lambert, L.S. , Edwards, J.R. & Cable, D.M. 2003. "Breach and fulfillment of the psychological contract: A comparison of traditional and expanded views". *Personnel Psychology*, 56(4), 895-934.
- Majchrzak, A., Rice, R.E., Malhotra, A, King, N., and Ba, S. 2000. "Technology Adaptation: The Case of a Computer-Supported Inter-Organizational Virtual Team". *MIS Quarterly*, 24 (4), 569-600.
- Markus, M.L., Majchrzak, A., and Gasser, L. 2002. "A design theory for systems that support emergent knowledge processes" *MIS Quarterly*, 26(3), 179-212

McAllister, D.J. 1995. "Affect and cognition-based trust as foundations for interpersonal cooperation in organizations" *Academy of Management Journal*, 31(1), 24-59.

McKnight, D.H., Choudhury, V. & Kacmar, C. 2002. "Developing and validating trust measures for e-Commerce: An integrative typology" *Information Systems Research*, 2002, 13(3), 334-359.

Menn, J. 2004. "Leaked code is traced to Microsoft partner firm". Los Angeles Times. Saturday February 14, p. C1

Peltier, T.R. 2001. *Information Security Risk Analysis*. Washington, D.C.: Auerbach.

Perrow, Charles 1999 *Normal Accidents Living with High-Risk Technologies*. 2nd Edition. NY: Basic Books

Rasmussen, E. 2004. *Application Security*. Presentation to the Marshall School of Business, University of Southern California, Los Angeles, January.

Rothke, B. 2001. "Corporate espionage and what can be done to prevent it". *Information Systems Security*, November/December,

Rousseau, D.M. 1995. *Psychological Contracts in Organizations: Understanding Written and Unwritten Agreements*. Thousand Oaks, CA: Sage.

Shih, S.C. & Wen, H.J. 2003. "Building E-Enterprise Security: A Business View" *Security Management*, September/October, pp 41- 49.

Schlarman, S. 2001. "The People, Policy, Technology model: Core Elements of the Security Process" *Information Systems Security*, November/December.

Sheppard, B.H. & Sherman, D.M. 1998. "The grammars of trust: A model and general implications" *Academy of Management Review*, 23, 422-437.

Walls, J.G., Widmeyer, G.R., and El Sawy, O.A.1992. "Building an Information System Design Theory for Vigilant EIS", *Information Systems Research* (3:1), 36-59.