Human Organization, Vol. 58, No. 3, 1999

0018-7259/99/030331-10$1.50/1

Dangerous Liaisons: Trust, Distrust, and Information Technology in American Work Organizations

Marietta L. Baba

This paper employs an inductive, natural-systems approach to explore the complex social and economic factors whose interaction generate trust and distrust between individuals, subunits, and firms in American corporations. The objective of this investigation is to gain a better understanding of the role of interpersonal trust and distrust on the implementation and use of new information technologies in organizational settings. The focus of the investigation is work-group control of information flow across organizational boundaries under conditions of trust and distrust, and the consequences of advanced information technology for such information-control practices. A central finding is that more powerful parties often try to force a shift in the medium of information exchange to gain greater control in specific hierarchical relationships. When these changes threaten the quality or security of information required by less powerful parties, resistance is the result. The discussion suggests that deployment of advanced information technology without the application of local knowledge of social interrelationships increases the risk of implementation failure.

Key words: trust, distrust, risk, information, information technology, electronic communication

Introduction

Relations of interpersonal trust in formal organizations are an emerging area of interest in the social and organizational sciences. Since economic transactions are embedded within networks of social relationships, the characteristics of those relationships—such as trust and its opposite, distrust—have a direct bearing on the effectiveness and efficiency of instrumental exchanges in organizational settings (Granovetter 1985). Trust between various organizational actors (including trust between individuals within a work group, in separate units within a firm, or in different firms) appears to confer a competitive advantage by enabling more effective cooperation and coordination among parties to an economic transaction (Fukuyama 1995). Where there is trust, different parties can enter into collaborative relationships more quickly, sustain coordinated action by making mutual adjustments, and learn from each other, rather than being bogged down for days, weeks, or months in formulating cumbersome contracts or building elaborate hierarchies that enforce a limited form of cooperation that ultimately may interfere with learning (Thompson 1967; Alter and Hage 1993). Organizational scholars and practicing managers alike have discovered that many economic objectives—from achieving success in mergers, acquisitions, and partnerships (Johnson and Lawrence 1988; Dodgson 1993; Kanter 1994) to creating new types of "virtual" organizations (Handy 1995) to sustaining the long-term economic growth and development of nations (Fukuyama 1995)—are furthered by high levels of trust in social and organizational relationships.

Prompted by competition from firms based in Japan and elsewhere in the East—where reciprocal bonds of obligation facilitate trust and cooperation between individuals and groups (e.g., Brunner et al. 1989)—American corporations have belatedly recognized the value of a trust-based "collaborative advantage" (Kanter 1994). In response, U.S. firms have adopted a number of new structures and management practices that attempt to build trust as a means to improve coordination and cooperation among parties representing different interests (e.g., employees and managers, managers of different subunits, firms and their customers, buyers and suppliers). These structures and practices include self-directed

Marietta L. Baba is professor of anthropology at Wayne State University. *The author is indebted to the research team at the Laboratory for Socio-Technical Systems Integration for gathering data that suggested the critical role of trust and distrust in electronic connectivity. Special thanks go to Allen Batteau and Wizdom Systems, Inc. for enabling access and field experiences that sharpened my awareness of the significance of trust in business relationships. I am also most grateful to employees in the automotive and aerospace industries whose personal stories of work and technology use vividly illustrated the issues discussed in this paper. Funding for the research reported here was provided by private-sector firms and government agencies that will remain anonymous. Any errors or omissions in this article are strictly the author's responsibility.*

and/or cross-functional work teams, total quality management, employee involvement, and category management (i.e., manufacturer-retailer partnerships), among others (Aoki 1990).

At the same time, American corporations also have pursued other pathways to a "collaborative advantage" that do not necessarily rely upon trust. Probably the most prominent of these are new information technologies such as electronic data interchange (EDI); computer-aided design (CAD), computer-aided manufacturing (CAM), and computer-aided engineering (CAE); shared databases; and computer supported cooperative work (CSCW) tools. Such technologies potentially offer many of the same advantages as trust; that is, they enable people based in different places and/or doing different jobs to coordinate their actions with greater speed and effectiveness. These benefits are believed to derive from the basic features of modern information technologies, which reduce the elapsed time for transactions, decrease error rates[1] and permit ease of collaboration with remote colleagues (via single-entry data points, automated electronic transmission, common access to shared databases, asynchronous and one-to-many communication networks (Davenport 1993; Sproull and Keisler 1993). Often, it is assumed that the deployment of new information technology will allow the corporation to circumvent or transcend geographical, temporal, cultural, or organizational barriers to cooperation, supposedly without the need for more intangible and difficult-to-manage changes in interpersonal relationships. Toward such objectives, American firms spent more than $400 billion on new computer hardware, software, and services in 1997 alone (David H. Hill, personal communication, July 11, 1999).

In American society, offering technological solutions to address economic, political, and social problems is not only commonplace, it is a distinguishing feature of our national culture (Segal 1985). The history of this society, a "civilized people on an uncivilized continent" (de Tocqueville 1862), coupled with conditions of severe labor shortage and serious labor-management conflict and violence over a number of centuries, established conditions that elevated the "technological fix" to the status of a managerial "silver bullet" (Baba et al. 1996). In American industry, new technology is viewed not only as a perfect substitute for labor (this idea is a cornerstone of economic theory), it can also take care of "people problems" by doing things people cannot or will not do, all with less hassle (see, for example, Hammer and Champy's 1993 arguments for technology-enabled "re-engineering").

While the success of information technology typically is not predicated upon bonds of trust, its failure often is the result of another phenomenon that has received less attention in the literature—distrust. Distrust is more than the absence of trust, it is the presence of particular cognitive and affective factors in the stream of social interaction that actively inhibit cooperation and coordination between different parties (McAllister 1995). The presence of distrust between firms, functions, and hierarchical levels in a corporation results from an expectation of harm that is based, in part, on the memory of past negative exchanges (actual or perceived) between particular groups (Luhmann 1988). Such expectations, warranted or not, may inhibit the sharing of information across group boundaries, which is a prerequisite for effective use of information technology (Sproull and Keisler 1993). Ironically, the absence of trust thus may indicate a potential blockage in one pathway to cooperation (i.e., information technology) that was not supposed to rely upon trust in the first place.

This paper employs an inductive, natural-systems approach to explore the complex social and economic factors whose interaction generate conditions of trust and distrust between individuals, subunits, and firms in American corporations. The objective of this investigation is to better understand the role of interpersonal trust and distrust on the implementation and use of new information technologies in organizational settings. A key focus of the investigation is work-group control of information flow across organizational boundaries under conditions of trust and distrust, and the consequences of new information technology for such information-control practices. The discussion will suggest that deployment of new information technology without the application of local knowledge of social interrelationships increases the risk of implementation failure.

Theoretical Background

The Concepts of Trust and Distrust

Until recently, trust and distrust were seldom subjects of systematic empirical investigation or theorizing by social scientists (Barber 1983). Management writers in particular often do not even define the words, or spend much time providing an anatomy of these concepts, presumably assuming that readers know what they mean. If one stops for a moment to consider the phenomena, however, it becomes apparent that the concepts of trust and distrust are not so simple. Complexity resides not only in the fact that different scholars have assumed different meanings for the terms (Hosmer 1995), but also that these concepts exist at multiple levels of analysis (individual, dyad, group, corporate entity), and have multiple dimensions. For example, in American studies of supervisor/worker and coworker dyads, trust has been found to have as many as five different dimensions, including (in order of importance) *integrity* (defined as honesty and truthfulness), *competence* (technical and interpersonal skill), *loyalty* (benevolent motives toward another), *consistency* (reliability, predictability, good judgment), and *openness* (willingness to share information and mental accessibility) (Butler and Cantrell 1984; Schindler and Thomas 1993). The relative importance of these factors in the United States, however, may differ according to the specific dyad one is examining. Openness, for instance, may be more important in horizontal or peer-to-peer dyads (e.g., between coworkers in a work group) than in vertical dyads, where other dimensions such as competence may be more critical.

Further, although trust and distrust are panhuman (i.e., they are an aspect of social relations in virtually all societies), they are defined and enacted differently in different cultural contexts. What constitutes trust, including its behavioral requirements and pre-conditions, is not the same in Japan or China as it is in the United States or Mexico. Fukuyama (1995) compares the sociocultural contexts of trust and distrust in several societies, including China, France, Germany, Italy, Japan, Korea, and the United States, showing that the willingness to trust various classes of persons in the economic sphere is related directly to differences in social structure and kin relations. An understanding of structural differences between the Japanese *ie* (household) and the Chinese *jia* (family), for example, is necessary to comprehend the reasons why trust relations in Japan may be extended to all of the members of a large corporate enterprise, while in China they are more typically limited to the kinship network. As cultures change over time, the meanings of trust and distrust also change. As an illustration, the requirements of trust rested more heavily on personal loyalty and obligations in the feudal societies of Western Europe than in their modern descendants, where technical competence is more critical (Barber 1983). Several writers have noted that, regardless of context, trust requires a shared system of values (see Hart et al. 1987). Thus, trust relations would be expected to be more likely between parties within a particular sociocultural group than between such groups.

A Definition of Trust

An emerging consensus among scholars suggests that trust may be defined as the subjective expression of one actor's *expectations* regarding the behavior of another actor (or actors). Trust exists when one actor expects that another will behave in such a way that the safety and security of the first actor will be preserved, under conditions in which the first actor is both *dependent* upon and *vulnerable* to the actions of the second, that is the first actor does not have control of the second, and there is the risk of harm (see Hosmer 1995).[2] Trust may be both a characteristic of a relationship between individuals or groups (e.g., a high level of trust in labor-management negotiations), as well as a characteristic of an individual (e.g., a child known to have a trusting character).

Two basic kinds of trust have been identified, each related to a different set of expectations about others (Barber 1983). The first kind of trust involves *general expectations* regarding the persistence and fulfillment of the natural and moral social orders. This is the form of trust we rely upon every day as we go about our routines—we trust the sun will rise in the morning and our family members will not harm us while we sleep. The second type of trust involves expectations that are *specific* to particular contexts and vary greatly from place to place. Specific trust is of two kinds, which are independent of one another: a) trust related to the technical *competence* of role performance; and b) trust related to *fiduciary responsibility*.[3] If we trust in the competence of another, we expect that he or she has the requisite knowledge, skill, and personal characteristics (e.g., dependability) needed to perform an action in a way that results in a positive outcome for us (e.g., we trust our surgeon to perform the operation in a competent manner). In the fiduciary form of trust, we expect that another will behave in a way that preserves and advances our interests while abstaining from opportunism (e.g., we trust our babysitter to make decisions about our children's welfare in a manner that, hopefully, benefits the children more than the sitter). This latter type of trust also has been called *goodwill*[4] (Dodgson 1993), based on the notion that fiduciary responsibility can extend beyond the call of duty, to inspire an actor to exploit opportunities that further another party's interests, while at the same time refraining from taking unfair advantage of the other.

Competence and fiduciary responsibility, respectively, may be related to two distinctive human foundations for trust: the cognitive and the affective (Lewis and Wiegert 1985). Trust is grounded in part on cognition-based criteria; we consciously choose those in whom we trust based on our perceptions of evidence for their trustworthiness (e.g., credentials, reputation, and demographics). Cognition-based trust thus may be related to competence. Affect-based trust reflects emotional investments in a relationship. When individuals demonstrate their genuine caring and concern for one another over time, there emerges a feeling in one that the other will do no harm. This aspect of trust appears to be connected to the notion of fiduciary responsibility. The two forms of trust, competence/cognitive and fiduciary/affective, function in distinctive ways, but may be causally related—the former may provide a foundation for the latter (McAllister 1995).

The Social Functions of Trust: Uncertainty and Risk

Trust has important functions in all societies, including the promotion of long-term stability (Cook and Wall 1980), reduction in the costs of exchange and other transactions (Schmidt and Posner 1982), and enhancement of the quality of life (Schindler and Thomas 1993). Trust is one way all societies deal with a central problem of the human condition—how to span the boundary between the self and the other, between us and them. Trust facilitates transactions needed for survival by reducing the *uncertainty and risk* (or complexity) of cooperation. Luhmann (1988) has emphasized the relationship between trust and risk. The existence of trust between two parties suggests that it is possible for one party to act in a way that could damage the other party, and that it is possible for the party at risk to therefore choose *not* to participate. The reason actors choose to enter into the risky situation is because of the bond of trust; without trust, the risk would be too great. Trust is a matter of probability, however, not certainty. There is always the possibility that expectations will be disappointed, even in the closest relationships.

The Concept of Distrust

The failure or absence of trust points to a related phenomenon—distrust. Distrust is not only the absence of trust, but the active expectation that other actors will behave in ways that do not ensure our safety and security. Luhmann (1988) pointed out that distrust is not only the opposite of trust, it is also a social *alternative* to, or *equivalent* of, trust. One can choose to trust or distrust, with each choice reducing social complexity. Distrust functions to identify situations in which we need to protect ourselves, and in this sense, it is an alternative mechanism of social control—it signals risk and reduces uncertainty by promoting avoidance of risk (Barber 1983). As a mechanism of social control, however, distrust has serious drawbacks. It consumes a great deal of energy, makes exploration of the environment very difficult, and may impede adaptive behavior (Hosmer 1995).

Distrust has been explored most thoroughly in the literature of economic exchange theory. The potential for self-interested or opportunistic behavior by agents with respect to principals, and the always-present risk of negative reciprocity found in short-term market transactions, have given many discussions of economic transactions a pessimistic flavor (Sahlins 1968; Plattner 1989; Hosmer 1995). The pessimism flows from the fact that it is very difficult to identify trustworthy agents or short-term trading partners. This literature, although pessimistic, makes clear the virtues of distrust. Under conditions where self-interested behavior by others is highly likely and difficult to avoid, distrust may be a necessary means of self-protection (e.g., caveat emptor). The connection between (dis)trust and economic exchange will become central in our later discussion of advanced information-technology use.

In organizations or in markets, risky economic transactions can scarcely be avoided, and considering the high costs of distrust as a mechanism of social control, societies have developed several other ways to mitigate against the consequences of incompetence and self-interest-seeking behavior. Anthropologists have noted the creation of rituals or other mechanisms that enable nonrelatives to become fictional kin, thus endowing a stranger with the quality of trust normally reserved for kinfolk, and facilitating economic cooperation (see Plattner 1989). In complex, industrialized societies, the importance of kinship as a built-in mechanism of trust is greatly reduced. Instead, the evolution of contract law and the emergence of insurance and warranty arrangements provide some assurance against risk where the trustworthiness of others cannot be determined in advance. Some writers have noted that these legal mechanisms create a special kind of trust, *contractual trust*, or the expectation that the other party will abide by the provisions of the contract, or suffer costly damages (Dodgson 1993). In organizations and the professions, hierarchies and policies for monitoring, auditing and controlling behavior, professional standards, and incentives for trustworthiness (i.e., use of reputation as a criteria for reward) have emerged to fill the need. These *substitutes for trust*, as they have been called, also carry large transaction costs, however, while providing no absolute guarantee that trustworthy behavior will result (Hosmer 1995).

Trust, Cooperation, and Power

An important debate in the literature concerns the relationship between trust and cooperation. Various writers have questioned whether trust is a prerequisite for, or a byproduct of, cooperation. Do employees need a high level of trust in management before they are willing to engage in employee involvement programs, or should management try to convince distrusting employees to participate, with the expectation that greater trust will result if management does indeed protect employees' interests during and after their participation? Bateson (1988) has shown that various animal species have evolved behavioral mechanisms that enable cooperation, apparently without trust, as it has been defined here. Humans also may engage in cooperation without trust. Axelrod's (1984) story of informal truces in the trenches called by soldiers on opposite sides of a military conflict is a vivid illustration. A more prosaic example is seen everyday as employees, some of whom undoubtedly do not trust their managers, troop to work and carry out managers' instructions. Under such conditions, however, there is not a complete absence of trust, nor is there full cooperation. The employees still must expect (trust) that they will receive a paycheck, or they will cease to show up. Further, the degree of cooperation that management can expect from distrusting employees is limited; indeed, this is one of the reasons why there has been so much interest in trust lately.

This discussion highlights the importance of another dimension of human experience in the trust equation—power relations. Power is defined as the capacity to produce intended and foreseen effects on others (Wrong 1995). The power holders in a given context often fill positions of fiduciary responsibility with respect to others, and the history of every society shows that the powerful often fail to discharge their responsibilities in a trustworthy manner. The collective memory of such violations and the distrust they engender often is what blocks the effectiveness of calls for change by power holders, when such change would require trust greater than that warranted by history. Organizational power dynamics are an especially salient dimension of the distrust that often impedes implementation of advanced information technology (AIT).

Social Distance, Exchange, and Information

Classic work in anthropology revealed long ago the inextricable connection between cooperative social and economic relations (e.g., Malinowski 1922). Sahlins's (1968) more recent discussion of reciprocity enables us to conceptualize the general relationship between trust as a social phenomenon and economic exchange. Sahlins identified three types of reciprocity—generalized, balanced, and negative.

Under conditions of *generalized reciprocity*, one party provides economic value to another on a relatively long-term basis without the requirement of payback. Such one-way "exchange" is predicated on a system of social obligations, moral values, and emotional attachments that compel one party to give to another without near-term compensation (e.g., relationships within the nuclear family; there may be an implicit expectation of return of similar value from some unspecified source at some unspecified time).

Contrasting with generalized reciprocity is another form of exchange quite familiar in Western society—*negative reciprocity*. In this form of exchange, one party attempts to best the other party by gaining through exchange something for which no compensation is offered. In other words, one party gets more than the other, or the exchange takes place at one party's expense. Relations in the marketplace often are used as an example of negative reciprocity. In such situations, there is often the opposite of trust, or distrust. Relations of power are especially relevant in situations of negative reciprocity. Those with greater power attempt to use their power (including the use of violence) to get the better end of the bargain, while those with less power exercise the power they do have to thwart this possibility. Given such struggles, distrust is likely to be an issue in exchanges involving parties of unequal power.

The type of exchange with the heaviest requirement for mutual trust outside the family is *balanced reciprocity*. Under this form of exchange, each party gives something of value to the other without the requirement for: a) immediate payback, or b) payback of exactly equal value. The exchange of value is both asynchronous and asymmetrical (e.g., you give me something now, I'll give you something different later). Despite this nonequivalence, the exchanging parties agree that, over the long term, the approximate value of their exchanges will be equivalent, and that the overall advantages of the relationship outweigh any slight differences in value that might be detected through careful quantification. Clearly, this type of relationship requires trust—both parties must expect that the other will not abandon them in the middle of the exchange cycle (Plattner 1989).

Our discussion of economic exchange suggests important roles for *information* and *social distance* in the development and maintenance of trust and distrust. Certain economic transactions carry greater risk because of the faultiness of available information (e.g., in short-term market transactions). Where there is insufficient high-quality information regarding: a) the nature of the goods or services to be exchanged; b) the rules of the transaction (e.g., price, terms); or c) the actors themselves, the risk of negative reciprocity will be greater (Plattner 1989). Under these conditions, long-term reciprocal relations, which generally reduce social distance between actors, are valued since they increase the amount and quality of information available and thereby minimize risk. This is why reciprocal transactions traditionally have been found among kinsmen, where social distance is small and access to information is large. On the other hand, if social distance is great, it is easier to take more than we give, since the other party is a stranger and we may never meet again. Greater social distance also results in less information being exchanged with the other party, meaning that it is more difficult to determine who is trustworthy and more difficult to build a relationship of trust. Thus, if the prior existence of distrust limits our contact with others, it may become self-perpetuating. Under such conditions, we will not engage in sufficient exchanges with others, nor gather enough information about them, to allow a relationship of trust to develop.

Risk, Distrust, and Information Technology

The social science literature links technology with both risk and distrust and emphasizes the importance of power relations in the links between these phenomena. Negative public perceptions regarding the risk of industrial technology, for example, have been related to a general distrust of authoritative institutions (government, science) and their managers (Laird 1989). Public perceptions of managerial incompetence, and perceptions regarding lack of fiduciary responsibility by those in positions of authority, both appear to be factors stimulating general public distrust of industrial technology.

The literature on information technology in organizational settings also points to the importance of risk and distrust. Shoshana Zuboff (1988), in her influential writing on the impact of computer technology on work, discussed the important shift from the world of physical reality to the world of symbolism represented by the diffusion of computing tools in the American workplace, and the distrust experienced by naive operators in their early encounters with computers. Because they did not yet understand the relationship between electronic symbols and the physical world with which they were familiar, nor the way in which such symbols represent more abstract variables and relationships, the operators' sense of certainty, competence, and control over the work process was shaken, with a resulting increase in psychological stress. In this situation, where computer-cause and real-world-effect were not clearly linked or understood, workers did not trust the computer to do what it was supposed to do and spent much time double checking the results of computerized commands. Managers tended to interpret such mistrust as an irrational expression of resistance to the technology when, in fact, the operators were not resisting the technology per se, but were compensating for their perception of increased risk of danger to their own work process by taking precautionary measures (a rational response).

Several writers have noted that the presence or absence of trust relationships between organizational managers and their employees are crucial factors shaping the process of new information technology implementation and its outcomes. When new information technology is viewed by managers as an opportunity to increase the pace of production, or the level of electronic surveillance over employees (e.g., by

monitoring their production through printouts or visual displays), decreased risk taking and innovation by employees can be the result (Zuboff 1982). Preexisting relations of distrust between managers and employees (and unions) also can increase the risk of failure in information-technology deployment (Majchrzak 1992), or otherwise make it difficult to reap the benefits of new information technology capabilities, such as virtual offices (see Handy 1995).

Sproull and Keisler (1993) raise another important issue that relates directly to information technology and (dis)trust; that is, the deliberate control of information to define, protect, and pursue work-group interests. In some corporate contexts, if a work group sends out completely accurate and thorough information, its strategic position vis à vis other groups may be compromised. Knowing this, work groups may deliberately misrepresent the information they send (e.g., "doctoring" the numbers to make their performance appear stronger), and recipients may discount the information they receive (e.g., a manager's suspicion that a work group inflated its cost estimates for a project to protect against cost overruns). Information technologies do not automatically change such tendencies, and thus do not ensure that information entered into an electronic system will be accurate or complete, or that it will not be misinterpreted. This means that information technology does not guarantee reductions in perceived risk or increases in trust between groups.

Sproull and Keissler's (1993) discussion focuses primarily on e-mail and electronic networking; does not consider the effect of other types of information technology (e.g., EDI, CAD/CAM) on intergroup exchange of information. While individuals and work groups have a relatively high degree of control over the content of e-mail messages, they are less free to alter the content of EDI or CAD/CAM, for example. Such technologies carry technical data that is defined more or less by an objective standard (e.g., prices and shipment dates, engineering design requirements, drawings of parts). When the content of electronic information cannot be altered freely, work-group efforts to control that information in pursuit of group interests may take forms other than misrepresentation and misinterpretation. Instead, as this paper will demonstrate, work-group struggles for information control may revolve around the *quality and security* of electronic versus physical forms of data, played out in terms of how the data is gathered and transmitted and who is given physical access to the data (discussed in detail in the case studies below). Such struggles often signal underlying issues of distrust between subunits, hierarchical levels, and corporate boundaries. It is toward a deeper understanding of these issues that we now turn our attention.

Case Data and Methods

The empirical window on trust provided by this paper views the phenomenon from the vantage point of a series of inductive case studies on advanced information-technology implementation in the automotive and aerospace industries. Data presented below are drawn from two separate multiyear studies of 19 work groups located in different divisions of U.S. automotive and aerospace firms, and the United States Air Force. The majority of these work groups were located in the Midwest. All the work groups either were in the process of, or had just completed, pilot tests or full-scale implementation of new computer-aided tools and/or redesigned work processes as part of a corporate effort to improve communication and cooperation between organizational units involved in new-product development. The types of work groups studied included product design, engineering support (e.g., transportation, purchasing), and manufacturing engineering. The membership of these work groups was overwhelmingly Anglo American and male.

Members of our multidisciplinary research teams spent a total of 24 months over a four-year period (1990-1994) observing work processes, attending meetings related to the implementation process, and talking in depth with work-group members and supervisors in the 19 work groups. In total, we spent approximately 500 hours in the field and conducted semistructured interviews with nearly 250 operations-level employees and their supervisors. For small work groups (less than 15 members), all or most of the employees were interviewed, either individually or in a group-interview format. For larger groups, a sample of employees stratified by age, role, and technological experience was interviewed. We also administered a survey on technology use and attitudes to 150 individuals across the work groups. For each work group, a structured set of comparative field data was collected, including the following:

1. Ethnohistorical material documenting the technological history of the work group and the larger division or company (for discussion of ethnohistory, see Baba 1988);

2. Map detailing the nature and steps of the work process before and after process change, developed by researchers using direct observation and one-on-one interviews with work group members (see Fetterman 1989; Werner and Schoepfle 1987);

3. Observational data capturing work group members' actual use of the new work process and technology;

4. Descriptive material on the general features of the transformation program as implemented at the work-group level, developed by researchers through interviews with transformation program managers and observation of implementation activities;

5. User evaluations of the new technology (from the emic or insider point of view), developed through the procedure described in Briody and Baba (1991) in which work-group members respond to open-ended questions about the benefits/advantages and costs/disadvantages of certain experiences; and

6. Survey questions administered on site to work-group members and supervisors, with questions focusing on attitudes toward work process and technology change.

Fieldnotes (including observation and interview data) were transcribed and stored electronically, and such data were analyzed using formal content-analysis techniques that permit the discovery of "native view" concepts and perspectives (i.e., emic coding; see Bernard 1988). Tally 3.0 software supported the content-analysis process (Pfaffenberger 1988). Propositions and hypotheses regarding factors that influence the implementation of new information technology were generated from this analysis process and were validated with work-group members and other stakeholders using ethnographic focus-group techniques (Morgan 1988).

Six Cases: Situational Background

Six cases in which trust was a major explanatory variable form the basis for our analysis and discussion (for additional cases see Baba 1995 and Baba et al. 1996.) In each of the six cases, relations of distrust—based on perceptions of incompetence and/or fear of breach of fiduciary responsibility—are the primary grounds for strong user objections to new information technology and the subsequent redefinition of technological objectives or outright rejection of the technology itself.

The cases are populated by a diverse array of organizational actors and relationships, but all are marked by interactions of social distance and exchange that create complex issues of risk and distrust. In each case, there are at least two and sometimes three discrete organizational work groups, with several types of boundaries among them. The types of focal groups and the boundaries separating them include: a) different functional work groups within a firm (Cases 2 and 6); b) hierarchically organized groups of managers and employees within a firm (Cases 3 and 4); and c) work groups in two different firms, especially firms in a buyer-supplier relationship (Cases 1, 3, and 5). In one case, more than one of these types is present (Case 3, which includes types b and c). Differential power relations across these types of work groups include those derived from status and prestige hierarchies among functions, for example, engineering and NC programming (Adler 1989); organizational authority hierarchies involving chains of command among mangers and employees; and relative buyer versus supplier power, based on differences in firm size and market dominance (Porter 1990).

Below are presented a series of brief synopses, providing the reader with a coherent sense of the distinctive story in each case. Unfortunately, limitations of space do not permit a full description of the data that would include the voices of people populating the cases. For ease of reference, the key features of each case (e.g., organizational actors, power relations, social distance, and risk and distrust issues) are summarized in Table 1.

Case 1: Transportation Group

A group of corporate engineers relied heavily on outside suppliers to support them in computer-aided design (CAD) of large containers used to transport their company's manufactured components. The engineers had selected carefully over several years a group of competent outside design houses to provide needed CAD designs on a contractual basis. Suppliers provided multiple services to the engineers, services that often went beyond the requirements of the contract (e.g., creative design solutions, and advice about materials to be used in construction and postretirement careers for the engineers). To facilitate interaction with the suppliers, the engineers purchased several different types of CAD equipment that were compatible with those used by the diverse population of suppliers; indeed, the suppliers had advised the engineers in these purchases. The corporation at which the engineers were based initiated a strategy to commonize all technologies used in new-product development as a means to enhance information flow and coordination between the numerous units working on new products. The engineers objected, fearing that their carefully nurtured group of suppliers would not be able to afford the expensive new tools, and that they might be forced to work with *other* supply houses—those who could afford the new technology and wanted the engineers' business, but could not be relied upon to provide the same kind of highly competent work and extracontractual benefits as supply houses of their own choosing. The engineers agreed to adopt one or two new CAD stations themselves, but refused to replace the seven different kinds of technology they used in designing components. This ensured technological compatibility with their chosen suppliers, but ironically worked against the goal of commonization.

Case 2: NC Programming

A group of NC programmers, which is paid an hourly rate to write computer programs for numerically controlled machines which cut parts for components, had been trying without success to implement CAD/CAM technology for a decade. Even though the group had tried on three occasions to integrate CAD/CAM tools into their work process, 80 percent of the group's work was still supported by paper blueprints and manual programming techniques.[5] The NC programmers did not use the electronic CAD design files available to them because they discovered that the files, created by CAD design groups located upstream from the NC programmers in the work process, contained minute flaws which, if undetected, could destroy the parts being cut by the machine and damage the machines as well. The source of the defects were tiny gaps between the surfaces represented in the design files. These nearly invisible gaps created no problems for the CAD designers, and since the designers had no direct contact with the NC programmers (i.e., they "threw the design files over the wall" to the programmers), there were no opportunities for designers to become aware of the problem. NC programmers were responsible for the quality of the NC programs sent to the machines, so to protect themselves, they decided to reenter all of the design data manually. Design engineers, learning of the programmers'

Table 1. Social Distance, Mode of Exchange, Distrust, and Risk in Six Cases

Case	Focal Work Groups	Power	Social Distance and Mode of Exchange	Distrust	Risk Posed by New Info. Tech.
1	•Corporate engineers •Suppliers in their network •Suppliers out of their network	•Buyer power over supplier •More or less egalitarian inside network	•Close social relations and balanced reciprocity within network (i.e., asynchronous flow of valued items over long periods); large distance and no exchange with suppliers outside the network.	•Fear of incompetence of suppliers outside the network; fear that outsiders will not provide extracontractual perks.	•New computers could disrupt an important means by which the balanced exchange is maintained technological compatibility; technological change could force acceptance of lower-quality information from outside the network.
2	•Design engineers •CAD designers •NC programmers	•Status/prestige hierarchy (high to low in column to left)	•Large social distance between engineers/designers and NC programmers (a social class difference); one-way negative flow of design files—flawed data "thrown over the wall," and then must be reentered manually.	•Engineers view programmers as incompetent; programmers view designers' data files as flawed.	•CAD/CAM will increase risk by forcing automatic acceptance of defective information that can damage parts and machines.
3	•Managers •Buyers •Suppliers	•Organization hierarchy •Buyer power over supplier	•Distance between firms required by legal/contractual mandate; potential for negative reciprocity between buyer and supplier (each tries to best the other).	•Managers distrust the technical competence of buyers, fearing they are "soft" on suppliers; both managers and buyers fear suppliers are not competent or honest.	•New computers will reduce the richness of information provided by on-site inspections, thereby reducing the quality of decision making by buyers; use of computers rather than field visits will reduce buyers' autonomy.

Table 1. Social Distance, Mode of Exchange, Distrust, and Risk in Six Cases (continued)

Case	Focal Work Groups	Power	Social Distance and Mode of Exchange	Distrust	Risk Posed by New Info. Tech.
4	•Managers •Inspectors	•Organizational hierarchy •Social class difference	•A large social and organizational distance separates managers and inspectors; they have a contractual relationship which provides for the exchange of wages for work (no guarantee of employment).	•Inspectors fear managers' incompetence in new technology implementation as well as a lack of fiduciary responsibility beyond the terms of the contract (i.e., managers won't protect, but instead will jeopardize inspectors' jobs). Inspectors also distrust computers' ability to do the required work.	•New computers will force skill obsolescence and thereby jeopardize the employment contract; inspectors do not know how to use the information provided by a CMM.
5	•Customer firm •Supplier firm	•Buyer power over supplier	•Distance between firms required by legal/contractual mandate; potential for negative reciprocity between buyer and supplier (each tries to best the other).	•Supplier fears buyer will violate confidentiality of a proprietary database.	•New electronic information exchange system could provide buyer access to proprietary data.
6	•Security officers •Other employees	•Status/prestige hierarchy	•Employees with different security clearances separated by rules on information sharing; potential for negative reciprocity (taking information without approval).	•Security officers fear breach of fiduciary responsibility by employees without proper security clearances.	•Use of e-mail or other electronic exchange systems could provide access to thieves or "enemy" hackers.

tinuing refusal to use the electronic CAD files, began to distrust the programmers' technical competence and sent their complex design jobs elsewhere (i.e., to places where, presumably, CAD/CAM was used effectively). This loss of work put the programmers' employment in jeopardy.

Case 3: Purchasing Group

A group of purchasing agents (called buyers) had responsibility for approving contracts between corporate engineering groups and outside design houses. It was the role of the buyer to certify that the supplier was charging the lowest possible cost and that the supplier had the facilities and skills to do the job as promised. The buyers made field visits to the suppliers' facilities, where they could "look the supplier in the eye" and inspect the facilities firsthand. Corporate management wanted to introduce a new computer system that would connect purchasing directly with the supply houses to enable computer-based audits rather than field visits. The purpose of the new system was twofold: a) to reduce the cost of audit by eliminating field visits; and b) to force buyers to study electronic blueprints of designs that would be provided via the computer. Management suspected that some buyers did not refer to technical data contained in blueprints before making contract decisions, relying more on subjective impressions and the suppliers' interpretation of the data (i.e., management did not trust its own buyers). The buyers protested that they would not be able to determine the work quality and cost accuracy of a supplier via computer; face-to-face interaction in the field was needed to validate a suppliers' capabilities and honesty. The inability to make field visits and the enforcement of blueprint reading also represented significant threats to the buyers' professional autonomy and competence. The ability to come and go between office and field was a mark of professional status in this organization. Further, many buyers did not have the background experience or skill needed to read a blueprint with competence. To protect themselves from these negative consequences, the buyers' technology evaluation team rejected the new systems based on "technical" adequacy.

Case 4: Supplier Quality Inspectors

A group of technical support personnel (i.e., inspectors) had the task of examining prototype parts created by outside supply houses and verifying the accuracy of these parts against technical specifications. Throughout their history, this group had used blueprints as the master standard against which the accuracy of suppliers' components were judged. Measurements were taken from the blueprints and then applied to the components, using various gauges and other physical measuring devices. Management wanted to increase the firm's ability to detect technical errors in supplier prototypes. They suggested that the inspectors give up their traditional tools and skills and do their jobs with more accurate tools—a computer-based coordinate measuring machine (CMM) that utilized mathematical design data. Unfortunately, virtually all of the workers in this group were computer illiterate. Further, there was no documentation available that explained exactly how to use the computer workstations to do the inspection job. To make the point that work objectives would be jeopardized by introduction of the new technology, the work group had created a list of 22 work tasks which could be performed using their traditional tools, but which (they believed) could not be achieved as effectively with computers. Management had assured the inspectors that they would be trained to use the new tools to do their jobs, but in interviews the inspectors expressed skepticism that this training would replace the skills and competency they already possessed. Indeed, the work group believed management would fail to provide sufficient instruction in the new technology, exposing the work group's computer illiteracy and thereby threatening their job security. As a result, the inspectors and their supervisors were able to delay implementation of the new system for several years.

Case 5: Prime Contractors

A contractor refused to purchase new computer-aided technologies so the firm could send electronic information on component designs and costs directly to its customer, the U.S. Air Force. They feared the customer, having open access to the supplier's databases, would give the design and cost information to competitors, enabling those companies to outbid the supplier on contracts. Rumors circulated regarding abuses that had occurred in the past. There also was the fear that access to cost data would enable the customer to pressure the supplier for lower prices, implying that the Air Force did not trust the supplier's integrity with respect to pricing. The supplier preferred to provide the customer with only very limited access to paper representations of design and cost information, in a highly controlled environment on the supplier's turf, with the supplier present. Replication of such issues at a number of contractor organizations impeded the Air Force's efforts to implement a "paperless" product-development process.

Case 6: The U.S. Air Force

Security officials assigned to a classified program in the U.S. Air Force, many of whom were computer illiterate, refused to allow any type of computer technology to be used as a communication device by civilian employees or military personnel working in the program. The security officials believed the security of computers could be breached by hackers who did not possess appropriate security clearances. Others believed the security officials also feared that the coming of computers could expose their own lack of knowledge of electronic security methods, thus making them look incompetent within in the organization. Only traditional forms of communication and transportation were to be used to send any kind of information related to a classified program (e.g.,

conencrypted telephones, armored trucks). Employees did not dare violate this ruling, since violation could result in a prison sentence. Employees also were prohibited from using electronic linkages to send information amongst themselves because of multiple levels of security clearance existing within the work group. People with higher-level security clearances were afraid they might send inappropriate information to a coworker with a lower-level clearance. To avoid the potentially serious consequences of such a breach, they avoided electronic communications altogether.

Discussion of Cases

Risk, Distrust, and the Control of Information

The case data suggest that *information control* is integral to social relations between work groups in organizations. Information is used, or deliberately not used, or even misused in various ways to *manage relationships* between work groups, both with those that are trusted and not trusted. With trusted others, the maintenance of valued information flows supports the competent performance of tasks and the protection of fiduciary obligations (i.e., Case 1, where the flow of information between parties was facilitated by cooperation in selecting compatible technologies to ease information flow). With distrusted others, however, a guarding against faulty information, and maintenance of the security of one's own information, ensures that one is not harmed by incompetents or those pursuing their own interests first (i.e., Cases 1, 2, 3, 5, and 6).

In cases of distrust, a key aspect of information control in the management of work-group relationships is *boundary maintenance*. When distrust exists between two work groups, social interactions between them tend to *create, perpetuate, and reinforce boundaries that maintain social distance*, either physical or symbolic (see Barth 1969). Numerous examples of boundary-maintaining distancing mechanisms were presented in the case material, including discrimination against and refusal to interact with certain parties (Case 1), throwing things "over the wall" and reentering data manually (Case 2), on-site audits (Case 3), rumors of dirty dealing by or incompetence of the other party, requirements for face-to-face review of data (Case 5), and differential security clearances and regulations (Case 6). The distance, and thus the boundary, are accentuated, elaborated, and maintained by such forms of distrustful interaction. Importantly, distancing mechanisms throw up barriers and filters to the free flow of information, either cutting it off completely (Cases 1 and 6), subjecting it to rigorous scrutiny under heavily guarded conditions (Cases 3 and 5), or filtering out some forms of information and only allowing in certain other narrowly defined forms (e.g., blueprints; Cases 2 and 4).

The introduction of new information technology creates problems for work groups because it can threaten to disrupt or destroy the boundary maintenance mechanisms used to manage intergroup social relationships. The risk of new information technology arises, in part, from the special characteristics of the technology itself, which create a number of challenges to information control by work groups. First, electronic communication may replace traditional boundary maintenance mechanisms, making them—and their means of controlling information—obsolete (e.g., Case 3, in which computers replaced field audits). Second, new technologies may remove the control of information from the local scene and place it in the hands of other parties (e.g., Case 5, where electronic data interchange would automate the flow of information between suppliers and buyers). Third, the new technologies represent information in an abstract form versus a physical form, whose security is easier to protect (e.g., Case 6, where computers were thought to be unsafe to transmit secret information, versus transmission via motor vehicle). Fourth, the new technology may be used to force a computer-based connection between a focal work group and an external information source deemed undesirable (Cases 1 and 2). The relative newness of the technologies in question means that some work groups have not yet developed effective ways to work around these "boundary busters," leading to various forms of "resistance to technology change," such as refusal to adopt or failure to use.

If the boundary is breached by new technology, the potential damage that can be done to a focal work group is quite serious. A powerful threat exists when new technology enables distrusted others to gain access to information that a focal work group may not want them to have, or prevents the focal group from getting information it needs. An equally serious threat exists when new information technology does not provide the quality of information needed by a focal group, under conditions in which the focal group is dependent upon high-quality information to perform its assigned work tasks. Significantly, the two types of potential risk—quality and security—each relate to one of the two fundamental dimensions of trust—competence and fiduciary responsibility, respectively. When the *quality of information is low*, a focal group could appear to be *incompetent* to those with whom a trust relationship is important (Cases 2, 3, and 4). When *the security of information is in jeopardy*, a focal group *risks injury from the self-interest seeking behavior* of distrusted ones (i.e., fiduciary responsibility is either absent or honored in the breach; Cases 5 and 6).

These two types of information-related risk—quality/competency and security/fiduciary responsibility—were evident across the six cases, as summarized below:

> In Case 1, *high quality information was an integral part of the reciprocal exchange network* between engineers and their trusted suppliers. A new medium of exchange (i.e., new technology) could potentially cut off exchanges within the network, while *forcing engineers to accept information of questionable quality* from suppliers they did not trust.
>
> In Case 2, the NC programmers rejected the CAD/CAM version of design data because they *distrusted the quality*

of the electronic information it contained. They *obtained greater control over the quality of information by using blueprints* and re-entering all the data themselves.

Case 3 showed that managers did not trust *the quality of information used by buyers to make decisions* (i.e., they did not use blueprints) and thus did not trust the buyers' competence. Buyers, on the other hand, believed the computer system *would reduce the quality of information received*, and the quality of decision making, while also threatening their autonomy and professionalism.

Case 4 revealed the reliance of inspectors on the information contained in blueprints, both to do their jobs and to maintain their employment contract with management. The new coordinate measuring machine *provided information that was useless* given their current skill level, and *management did not provide access to information* that might have bridged the knowledge gap.

In Case 5, suppliers maintained strict physical security over their confidential data by insisting they be present whenever it was examined by the buyer. A new automated data exchange system threatened that a powerful buyer would be able to *access and misuse proprietary design information and also access cost information that could reduce the supplier's future revenues.*

Case 6 found security officials forbidding certain media of information exchange, based on the belief that these media were susceptible to hackers who would *gain access and use information gained to harm the agency.*

It is these kinds of risks that the focal work groups were trying to minimize or manage through the establishment of boundary maintenance mechanisms, and it is the fact that electronic communication reintroduces these risks that causes work groups to resist new information technology.

As noted in the foregoing, the issues of security and quality affect both work-group relationships of distrust *and* trust. Conditions that threaten to disrupt a relationship of trust are just as dangerous, if not more so, than those that threaten to force a closer relationship with the distrusted. While a sense of distrust is a signal to use greater caution, there is little that can be done immediately to compensate for the loss of a trust relationship. Figure 1 provides the following summary of how quality/competency and security/fiduciary responsibility issues create risks for relations with *both* the trusted and the distrusted:

Cell 1. Distrusted others will not protect our interests. Distrusted others will access too much information, which they can abuse, or will not give us the information we need to prevent abuse (Cases 3, 5, and 6);

Cell 2. Distrusted others may be incompetent. The focal work group obtains information that may not be accurate or otherwise high in quality (Cases 1 and 2);

Cell 3. We will not be able to fulfill our responsibility to trusted others. Existing fiduciary relationships between the focal group and trusted or valued others could be disrupted (Cases 1 and 3); and

Cell 4. We appear incompetent to trust others. Low-quality information makes focal group appear incompetent to others whose opinion is valued (Cases 2, 3, and 4).

We now turn our attention away from information technology per se as a source of risk and consider another critical factor that can threaten work-group control of information—hierarchical relations of power inside organizations.

Figure 1. Information Technology and Relations of Trust and Distrust

	Fiduciary Responsibility	Competence
Distrusted Others	1. Access to too much, or not enough, info can lead to abuse	2. Info may be inaccurate or low in quality
Trusted Others	3. Existing relationship of responsibility is jeopardized	4. Appearance of incompetence

Power Relations and Technology Change

Technological risks to competency and fiduciary responsibility exist both for those with relatively greater power, and those with relatively lesser power, in a given organizational context. The powerful may fear the incompetence of less-powerful others, as in Case 2 where the engineers attempted to avoid the perceived incompetence of the NC programmers by sending complex jobs elsewhere. The less powerful also may have such fears regarding the powerful, as in Case 4 where the workers feared the managers' incompetence with respect to new technology implementation. Both the more and less powerful also worry about breach of fiduciary responsibility: in Case 3, both the managers and the purchasing agents worried about others who might fail to protect the firms' best interests. Those with relatively greater power may be afraid of appearing incompetent to others (as in Case 6 where the security officials may not have been competent to determine the safety of electronic communication), as may be the less powerful (in Case 4, the workers were afraid of losing their skill-based competency). Finally, both the more and the less powerful are concerned about their ability to fulfill fiduciary obligations to others. In Case 3, the purchasing agents—who were relatively less powerful than management—still wanted to protect their firm from supplier fraud. Thus, it is not necessarily one's position in a power hierarchy that determines the type of trust issue one confronts with the introduction of new information technology.

What is more significant is the way more- or less-powerful work groups maneuver to gain advantage over others during the introduction of new information technology. The cases show that more powerful parties often try to force a shift in the medium of information exchange *to gain greater control in a specific relationship*. This was seen in several cases (3, 4, and 5) where management or a powerful buyer tried to change the medium of information exchange to better control employees or their suppliers. Unfortunately, these changes often threaten the quality or security of information required by the less powerful party. When this happens, the less-powerful party uses its own power to resist.

One interesting pattern that emerges from the cases is the unwitting role played by the powerful in the scuttling of their own plans. In all cases, changes in information technology were initiated by higher-level corporate executives as a means to streamline costs and cycle time across the firm as a whole, or they were initiated by powerful buyers vis à vis weaker suppliers as a means to the same objectives. Across all cases, resistance to technology change was derived primarily from conditions of distrust that created certain explicit risks in the eyes of the less-powerful group.

Significantly, the more powerful ones often were implicated directly in creating the existing conditions of distrust in the first place. In Case 2, it was the relatively more powerful group of designers that sent flawed data to the programmers. In Case 3, management distrusted the competence and fiduciary responsibility of its own buyers. In Case 4, management was distrusted by inspectors because of its past practice of downsizing during technology change. In Case 5, the powerful buyer was reputed to have inappropriately handled other suppliers' proprietary data in a way that damaged those suppliers. In all these cases, the prior actions of a more powerful party created conditions of distrust which, in turn, generated resistance to technological changes introduced by those with greater power. Powerful agents whose technology change initiatives require *others* to alter their modes of operation and interaction in significant ways do not appear to recognize that such changes also require increased levels of trust in exchange relationships. Yet, ironically, higher levels of trust often cannot be achieved or sustained because of historically grounded expectations of distrust for which the more powerful are, at least in part, responsible.

Implications for Theory and Practice

The literature generally does not fully recognize the role of information and information technology in the maintenance and management of social and economic relationships within and among organizations (see Fukuyama's 1995 review). Anthropological discussions of reciprocity emphasize the importance of information as a decision criteria in managing economic exchanges but give limited attention to transactions in which *information itself* is the object of exchange. Profound changes in the nature and control of information introduced by advanced information technologies (AIT) alter the rules of the exchange game by reducing social distance across time and space, and by shifting the locus of control away from local and toward more global decision makers (i.e., more centralized or hierarchical authorities). Work groups may, in effect, be forced to enter into transactions in which the object of exchange (i.e., information) can itself be quite dangerous, whether in "give" or "receive" mode. Theories of reciprocity need to be reconceptualized to accommodate the exchange of information under such conditions.

With respect to corporate policy and practice, decision makers should recognize that the increased risk represented by loss of control over boundary maintenance can fly in the face of simultaneous efforts to encourage cooperation across work groups. The culturally embedded nature of trust and distrust, however, means that it will not always be possible to determine in advance how a specific information technology will affect existing social networks and boundaries. The cases presented here show that these influences are culture-specific. Gaining such knowledge will require a new form of cultural risk assessment, one that leads to an understanding of the role of social relations in current work processes and the changes that should be expected given technology deployment plans. Such an assessment process would be necessary to identify existing networks of trust and prevent their destruction in the change process.

Another important implication for corporate policy and practice concerns the role of power in the process of building greater cooperation and trust. In the cases examined earlier, those with greater power sometimes initiated actions that would have increased the level of risk borne by others. In Case 3, for example, management wanted to increase their control over buyers without regard for the buyers' professional requirements, and in Case 4 management sought to improve the precision of inspections without concern for the obsolescence of inspectors' skills. The effect of these actions was to heighten a sense of distrust among the less powerful, thwarting management initiatives. Perhaps those with greater power should try an inverse action to reduce distrust; that is, they should initiate actions that increase the level of risk borne by *themselves*. For example, top management could provide employees with access to sensitive financial information or guarantee (and fulfill) employment security in the face of crisis. The logic here is that acceptance of greater risk by more powerful parties breaks the self-perpetuating cycle of negative reciprocity by extending to the less powerful something of significant value without requiring something of equal or greater value up front; thereby, initiating an exchange cycle that more closely resembles generalized or balanced reciprocity rather than negative reciprocity. Such a risky move by the powerful could reduce social boundaries and encourage a response of balanced reciprocity from employees (e.g., an increased level of participation).

Conclusion

Under conditions of global competition, strategic management in American work organizations is attempting to counter decades of self-interest-seeking behavior across functions and units by promulgating policies and practices that encourage greater cooperation and trust. The American penchant for technological solutions has led to the emergence of a multibillion-dollar industry that offers new information technologies partly as a means to achieve the desired cooperation in a way that is certain, fast, and requires few changes in organizational management. Unfortunately, these "technofixes," instead of solving the boundary problem, often fall victim to it. Informal means of relationship management, created spontaneously by work groups as a way to achieve their objectives and protect themselves from harm, form a deeply rooted and tenacious social infrastructure that is not easily brushed aside by technology alone. The possibility of significant change in American work organizations requires new economic theories of the firm, as well as new concepts of organization and management, that accord natural social relationships the status they warrant as a powerful and generative dimension of organizational capability.

Notes

[1]Errors are reduced because information need be entered only once into the system, thus reducing the likelihood of mistakes that accompany multiple entry points. The high dependability of information technology greatly reduces processing errors.

[2]Gambetta (1988) defines trust as the particular level of subjective probability that one social actor assigns to the likelihood that another actor will perform a particular action, both before the first actor can monitor the other actor and in a context where the action affects the first actor.

[3]Fiduciary in this context is defined as a relationship in which one party has been designated to represent the interests of a second party, and the first party does so in a manner that puts the second party's interests ahead of the interests of the first party.

[4]In business, goodwill is defined as "an amount paid by one firm in acquiring another business enterprise that is greater than the sum of the then-current values assignable to individual identifiable assets" (Stickney et al. 1991:58). This amount derives in part from the firm's reputation for trustworthiness in past dealings with others. This notion again points to the economic value of trust.

[5]In CAD/CAM, design information flows directly from the CAD design group to the NC machines where parts are cut; no blueprints are used, and the machines are programmed electronically.

Refereces Cited

Adler, Paul
1989 CAD/CAM: Mangerial Challenges and Research Issues. IEEE Transactions on Engineering Managment 36:202-215.

Alter, Catherine, and Jerald Hage
1993 Organizations Working Together. London: Sage.

Aoki, Masahiko
1990 Toward an Economic Model of the Japanese Firm. Journal of Economic Literature 27:1-27.

Axelrod, Robert M.
1984 The Evolution of Cooperation. New York: Basic Books.

Baba, Marietta
1988 Two Sides to Every Story: An Ethnohistorical Approach to Organizational Partnerships. City & Society 2:71-104.

1995 The Cultural Ecology of the Corporation: Explaining Diversity in Work Group Responses to Organizational Transformation. Journal of Applied Behavioral Science 31:202-233.

Baba, Marietta, Donald Falkenburg, and David Hill
1996 American Culture and Technology Management: Implications for Business Process Re-Design. Research Technology Management 39:44-54.

Barber, Bernard
1983 The Logic and Limits of Trust. New Brunswick, N.J.: Rutgers University Press.

Barth, Fredrik
1969 Ethnic Groups and Boundaries. Boston: Little, Brown, and Co..

Bateson, Paul
1988 The Biological Evolution of Trust. *In* Trust: Making and Breaking Cooperative Relations. Diego Gambetta, ed. Pp. 14-30. New York: Basil Blackwell.

Bernard, H. Russell
1988 Research Methods in Cultural Anthropology. Newbury Park, Calif.: Sage.

Briody, Elizabeth, and Marietta Baba
1991 Explaining Differences in Repatriation Experiences: The Discovery of Coupled and Decoupled Systems. American Anthropologist 93:322-344.

Brunner, James, Jiwei Chen, Chao Sun, and Nanping Zhou
1989 The Role of Guanxi in Negotiations in the Pacific Basin. Journal of Global Marketing 3:7-22.

Butler, John K., Jr., and R. Stephen Cantrell
1984 A Behavioral Decision Theory Approach to Modeling Dynamic Trust in Superiors and Subordinates. Psychological Reports 55:19-28.

Cook, John, and Tobi Wall
1980 New Work Measures of Trust, Organizational Commitment, and Personal Need Nonfulfillment. Journal of Occupational Psychology 53:39-52.

Davenport, Thomas
1993 Process Innovation: Reengineering Work through Information Technology. Boston: Harvard Business School Press.

de Tocqueville, Alexis
1862 Democracy in America. London: Longman, Green, Longman and Roberts.

Dodgson, Mark
1993 Learning, Trust, and Technological Collaboration. Human Relations 46(1):77-95.

Fetterman, David M.
1989 Ethnography, Step by Step. Newbury Park, Calif.: Sage.

Fukuyama, Francis
1995 Trust: The Social Virtues and the Creation of Prosperity. New York: Free Press.

Gambetta, Diego, ed.
1988 Trust: Making and Breaking Cooperative Relations. New York: Basil Blackwell.

Granovetter, M. S.
1985 Economic Action and Social Structure: The Problem of Embeddedness. American Journal of Sociology 91:481-510.

Hammer, Michael, and James Champy
1993 Reengineering the Corporation: A Manifesto for Business Revolution. Cambridge, Mass.: Harvard Business School Press.

Handy, Charles
1995 Trust and the Virtual Organization. Harvard Business Review 73:40-50.

Hart, K., H. Capps, J. Cangemi, and L. Caillouet
1987 Exploring Organizational Trust and Its Multiple Dimensions: A Case Study of General Motors. Organizational Development Journal 4:31-39.

Hosmer, Larue T.
1995 Trust: The Connecting Link Between Organizational Theory and Philosophical Ethics. Academy of Management Review 20:379-403.

Johnston, Russell, and Paul R. Lawrence
1988 Beyond Vertical Integration—the Rise of the Value-Adding Partnership. Harvard Business Review 66:94-101.

Kanter, Rosabeth Moss
1994 Collaborative Advantage. Harvard Business Review 72:96-108.

Laird, Frank N.
1989 The Decline of Deference: The Political Context of Risk. Risk Analysis 9:543-550.

Lewis, J. D., and A. Weigert
1985 Trust as Social Reality. Social Forces 63:967-985.

Luhmann, Niklas
1988 Familiarity, Confidence, Trust: Problems and Alternatives. *In* Trust: Making and Breaking Cooperative Relations. Diago Gambetta, ed. Pp. 94-108. New York: Basil Blackwell.

Majchrzak, Ann
1992 Management of Technological and Organizational Change. *In* Handbook of Industrial Engineering. Garriel Salvendy, ed. Pp. 767-797. New York: John Wiley.

Malinowski, Bronislaw
1922 Argonauts of the Western Pacific. New York: Dutton.

McAllister, Daniel
1995 Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. Academy of Management Journal 38:1, 24-59.

Morgan, David L.
1988 Focus Groups as Qualitative Research. Newbury Park, Calif.: Sage.

Pfaffenberger, Bryan
1988 Microcomputer Applications in Qualitative Research. Newbury Park, Calif.: Sage.

Plattner, Stuart
1989 Economic Anthropology. Stanford, Calif.: Stanford University Press.

Porter, Michael
1990 The Competitive Advantage of Nations. New York: Free Press.

Sahlins, Marshall
1968 Tribesmen. Englewood Cliffs, N.J.: Prentice Hall.

Schindler, Paul L., and Cher C. Thomas
1993 The Structure of Interpersonal Trust in the Workplace. Psychological Reports 73:563-573.

Schmidt, Warren, and Barry Posner
1982 Managerial Values and Expectations: The Silent Power in Personal and Organizational Life. New York: American Management Association.

Segal, Howard
1985 Technological Utopianism in American Culture. Chicago: University of Chicago Press

Sproull, Lee, and Sara Keisler
1993 Connections: New Ways of Working in the Networked Organization. Cambridge, Mass.: MIT Press.

Stickney, Clyde P., Roman L. Weil, and Sidney Davidson
1991 Financial Accounting. Fort Wayne, Ind.: Harcourt, Brace and Jovanovich.

Thompson, James D.
1967 Organizations in Action. New York: McGraw-Hill.

Werner, Oswald, and G. Mark Schoepfle
1987 Systematic Fieldwork. Newbury Park, Calif.: Sage.

Wrong, Dennis Hume
1995 Power: Its Forms, Bases and Uses. New Brunswick, N.J.:Transaction.

Zuboff, Shoshana
1982 New Worlds of Computer-Mediated Work. Harvard Business Review 60:142-152.
1988 In the Age of the Smart Machine. New York: Basic Books.