CERIAS Tech Report 2006-35

TRUST, RISK, AND ECONOMIC BENEFITS IN ONLINE ENVIRONMENTS

by Fariborz Farahmand, Shari Lawrence Pfleeger, Eugene H. Spafford

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Trust, Risk and Economic Benefits in Online Environments

Fariborz Farahmand
Krannert School of Management
Purdue University, West Lafayette, IN 47907-2056
fariborz@purdue.edu

Shari Lawrence Pfleeger
RAND Corporation, 1200 South Hayes Street, Arlington, VA 22202-5050
Shari_pfleeger@rand.org

Eugene H. Spafford
Center for Education and Research in Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086
spaf@purdue.edu

Lack of trust is identified as one of the main constraints on online environments, particularly in terms of consumer protection. Although the elements that contribute to building trust can be identified in broad terms, there are still many uncertainties in defining and establishing trust in online environments. This paper investigates these uncertainties by studying the relationship between trust and the risk perceptions of users. We discuss issues such as trust as an economic good, risks to procedural fairness, and the relationship between the two. We posit that without an organizational policy governing fair use of personal information, organizations face the risk that information used inappropriately by a single employee or by a single department can have negative consequences for the entire firm. We stress the need for organizations to consider user perceptions of risk when establishing trust with their customers, and we show that economic decision-making in online environments without consideration of trust and risk is not likely to result in optimal choices.

Keywords: cyber security, economics, perception, policy, positional good, risk, trust

---

1. Introduction

Online environments provide a venue for people and organizations to perform many activities, including:

- Providing, gathering and sharing information,
- Meeting and interacting with others, and
- Performing transactions of various kinds.

This work was supported by the Economics of Cyber Security project of the Institute for Information Infrastructure Protection (I3P) under award number 2003-TK-TX-0003 from the Office for Domestic Preparedness/Office of Justice Programs and the Department of Homeland Security.

Inherent in each of these activities is some type and level of trust. We can think of trust in at least three ways, corresponding to the three pillars of cyber security (Pfleeger and Pfleeger 2007):

- *Confidentiality*: Online actors trust that information (particularly identity) will be kept confidential when such confidentiality is promised.
- *Integrity*: Online actors trust that information posted is correct, and that information provided by the actor will not be changed or falsely attributed.
- *Availability*: Online actors trust that information and systems will be available when needed.

Indeed, online trust has economic benefit: people and organizations will pay to ensure a desired degree of trust. However, high degrees of trust can be expensive, as evidenced by resources devoted to preventing cyber attacks, monitoring computer systems, detecting unwanted behavior, mitigating the effects of attacks, and cleaning up the problems they cause. For this reason, online actors often determine (intentionally or not) an acceptable balance between trust and risk. In this paper, we explore the relationship among trust, risk and economic behavior. We show that, to understand trust and risk in online environments, we must understand the multidisciplinary nature of cyber security economics and online behavior.

2. The Meaning of Trust

Trust necessarily involves two parties: one who is *trusted*, and one who is *trusting*. Thus, we can think of each party as having two trust-related characteristics: being trustful (i.e. willing to trust another person or organization) or being trustworthy (i.e. engendering the trust of someone or something else). (Pelligra 2005) Moreover, trust can characterize relationships within an organization as well as those crossing organizational boundaries. To see how trust functions online, we first explore notions of trust in general.

How do individuals construct a basis for trust? One traditional answer to this question is that people search for signs of objectivity and fairness, and perhaps also for signs of competence and expertise. According to this formulation, a person who is judged trustworthy by one should be judged trustworthy by all (Earle 2004). The alternative approach contends that trust is based on specific, locally defined manifestations of similarity and agreement rather than on universally accepted criteria. This formulation contends that trustworthiness is a matter of individual judgment that varies across persons, contexts, and time.

We often consider trust as a function of civil and criminal law, but in fact it also derives from the norms of a civil society. These norms are conveyed in interpersonal interactions, often moderating or preventing negative behaviors, such as fraud. For example, (Rabin 1993) has shown that payoffs depend not only on players' actions but also on their intentions. The intention is determined not only from what players do but also from what they can do but do not. Norms can act to deter a player from taking an unpopular, unethical or even illegal action. In cyberspace, norms are sometimes difficult to determine, but online trust certifications and systems (such as eBay assurances, Better Business Bureau ratings, or amazon.com reviews) attempt to capture actor behavior and provide surrogate measures of trust. Similarly, jargon is related to normative group expectations. Shared meanings, specialized terminology, and the consonance of assumptions underlying group discussions can lead to familiarity and trust among team members. (Gui 2005) Such shared terminology is often found in listservs or specialized web sites.

Several researchers highlight characteristics that can affect whether and how we trust a person, good or service. Baker (1987) and Jones (1996) suggest that trust is a personality trait, and Baier (1986) and Gambetta (1988) claim that there is an element of probability involved when one person or organization decides to trust another. Pelligra (2005, p. 113) makes a convincing argument that interpersonal relationships create and enhance trust:

> "A trusting move induces trustworthiness through an endogenous modification of [someone's] preference structure. A single act of genuine trust may provide additional reasons to behave trustworthily."

Pettit (1995) describes how traits displayed by the party to be trusted are determined by self-interest: e.g., the desire to be admired by others. As trust become more valued, it grows.

> "Following the norm of trust has an effect on both the beliefs and the norms of others. It creates a virtuous circle … if we act as if we expect the best from the others, they will often behave better as a result." Baron, (1998, p.411).

This need to be thought well of by others is also called "therapeutic trust." Horsburgh (1960, p. 346) describes how it affects economic decisions: "One of the reasons for [A's] willingness to risk the loss of his money is a belief that this may induce [B] to act more honorably than he originally intended."

3. Trust as an Economic Good

Trust and its associated characteristic, legitimacy, are important and related constructs that affect economic relations between individuals and organizations. Legitimacy is a particular kind of trust that can determine how firms interact with one another. When Aldrich and Fiol (1994) examined the difficulty associated with being a new firm in a new industry, they found that one of the largest challenges was a lack of legitimacy. This finding contrasts with traditional economic theory, which asserts that firms decide whether to enter or exit markets based on the risks and trade-offs of the decision. Moreover, legitimacy can affect the terms of exchange in bargaining situations. Because regulators and the media are much more likely to confer legitimacy on firms that fit the common image of organizations in their field, firms tend to behave alike (Deephouse 1996).

In cyberspace, legitimacy is signaled by association with membership groups such as the Institute of Electrical and Electronics Engineers (IEEE), through credentialing systems such as the Certified

Information Systems Security Professionals (CISSP), or by conforming to the Software Engineering Institute's Capability Maturity Models (SEI-CMM). Somewhat paradoxically, the process is sometimes more useful for signaling legitimacy—for example, in the context of government software contracts—than it is for actually improving the factors that could enhance that legitimacy, such as improving software quality outcomes.

Economists call trust a *positional good*, because people are willing to pay more for goods and services they trust. It is positional in that we can say that one entity is more trusted than another, and position in the marketplace can be influenced by the degree of trust. Moreover, trust plays out in economic interactions through interpersonal relationships. By this, we mean the "forms of human interaction in which the identity of the participants as particular human beings has affective or cognitive significance." Gui and Sugden, (2005, p. 2).

> "Conventional economic theory models the behavior of rational agents, characterized only by, and motivated only by, their preferences and beliefs; in consequence, it recognizes only the cognitive dimensions of interaction between its agents. This methodological strategy, one might say, treats all interactions as impersonal. In contrast, a recurrent theme in recent work on economics and social interaction is the idea that interpersonal interaction involves the communication of dispositions or sentiments that are affective or visceral in nature." (Gui and Sugden, 2005, p. 13).

Gui and Sugden (2005b) suggest two reasons why trust in interpersonal relations matters for economics. First, when trusting relationships occur inside an (economically-based) organization, they can affect economic performance by reducing both the time and the cost of a transaction. This activity is evident in many ways related to cyber security. For instance, usually less stringent technical monitoring and protections are needed when the organization's members know and trust each other. Second, when good relations occur outside the organization, trust can encourage strong economic performance by providing "material and emotional support for starting entrepreneurial initiatives." (Allen 2000). Trust can

lead to faster economic growth (Zak and Knack 2001), and trusted interpersonal relationships can become channels for sharing and transmitting economically valuable information (Topa 2001).

However, McAllister (1995) found that although good personal relationships are associated with higher levels of trust, a history of competence, reliability, and even credentials are necessary for gaining trust in organizations. Recognition of these qualities typically precedes strong interpersonal relationships. Jones and George (1998) suggest that, in addition to trusting in people's abilities, understanding other workers' intentions led to better organizational performance by improving knowledge exchange, involvement, and communication of tacit operating procedures.

4. Risk Management in Various Industries and Business Sectors

Risk is defined as the possibility of loss, injury, disadvantage, or destruction (Webster 1986) and its relevance varies over various industry segments (Daniels and Spafford 1999). Many different approaches to risk management are used in business and government sectors, including general business, banking, environmental agencies, and medical services. This section presents a brief review of some of the more relevant approaches.

A typical approach for project management in general is presented by Mundt, who describes a 3-dimensional *constraint matrix* that represents the impact of each risk, the likelihood that it will occur, and the difficulty in detecting it (KPMG 2005). Shtub et al. (1994) discusses the major steps of risk management as consisting of 1) risk identification, 2) risk quantification, 3) risk response development, and 4) risk response control. Smyth presents a *decision tree* approach to recommend building modifications to minimize damage from earthquakes (Smyth 2003). A probabilistic approach is used to estimate changes in damage from different *levels* of structural strengthening. The decision tree approach is well known for its applicability to a variety of decision-making situations (Raiffa and Schlaife 1961). However, its application to specific problems requires much care and considerable experience. For example, Kunreuther (2001) discusses the problems of risk assessment and risk perception for extreme or

rare events. He recommends the use of *exceedance probability curves* for use in the assessment process. For other situations, *fault tree analysis* is an elaborate version of the decision tree approach used for reliability analysis of systems involving hardware, software, human involvement, and environmental factors (Henley and H. Kumanota 1981, Kapur 1982).

Multi-attribute utility (MAU) functions represent another approach (Keeney and Raiffa 1976). The challenge in applying MAU is to develop the trade-off curves among risks, costs, and other relevant factors.

Muermann (2002) differentiates between the credit and operational risk to a financial organization. Credit risk can be approached with *statistical methods*, and high-risk clients can be charged higher loan interest rates. Similarly, firms can engage in currency hedging and interest rate swaps to protect against well-known dangers. For operational risks, which are idiosyncratic and less frequent but threaten potentially greater damage, a different approach is needed. In this case, classifying the risks reveals the underlying risk structure. An internal definition process is proposed, whereby banks dynamically adjust to new incidents.

For the insurance industry in the UK, a three-dimensional approach is recommended that reflects

- Consequences – Both threats and opportunities,
- Probability of occurrence – Threats, and
- Probability of occurrence – Opportunities (IRM 2002).

A range of techniques is recommended for performing the detailed analysis, including event tree analysis, statistical inference, and real options, but no examples are provided. Kleindorfer (2004) presents an approach to dealing with environmental damages with reference to the Clean Air Act Amendment. He describes *statistical associations* among facility characteristics, accident rates and severity, regulatory programs in force, community demographics, and the debt/equity ratio of the parent company. The results of such a statistical analysis can be used to guide preventive and corrective actions. A similar approach is described by Elliott for statistical associations between county demographics and the accidental release of

toxic or flammable chemicals in facilities located in those counties (Elliott 2004). Abdel-Rahman (2000) discusses a similar approach for deciding on actions to address potential ecological damage to both wildlife species and humans. The methodology includes the steps of 1) problem formulation, 2) toxicity evaluation, 3) exposure estimates, 4) risk calculations, and 5) assessment endpoints.

Michel-Kerjan (2002) discusses more complex situations involving infrastructure networks and interdependent networks, where a global approach is needed to address such threats. He cites several examples, among them: The loss of hydro-electric power in Quebec Province in 1998 as an example of an unforeseen disaster that required unprecedented mitigation efforts, and the failure of the international communications satellite Galaxy IV, which caused 45 million pagers and 600 radio stations to stop working. Such vulnerabilities present unique challenges in prediction and loss prevention.

One of the other factors that can affect an organization's attitude towards risk is its basic risk tolerance. Broadly defined, risk tolerance is the amount of risk an organization is willing to accept in pursuit of value [CSO 2004]. That is, risk tolerance can be defined as the amount of risk an organization is able to accept, manage, and optimize effectively (McCarthy and Flynn 2004). It reflects the organization's risk management philosophy, in turn based on the organization's culture and operating style. An organization's risk tolerance in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks, can be measured either qualitatively or quantitatively:

- Quantitatively: The risk is calculated using the normalized certainty equivalent. The analyst determines the decision maker's attitude toward risk by performing a utility analysis, or by assessing historical actions of the business in practice. For example, Howard (1988) defines certain guidelines for determining a corporation's risk tolerance in terms of total sales, net income, or equity. According to Howard, reasonable values of risk tolerance appear to be approximately 6.4 percent of total sales, 1.24 times net income, or 15.7 percent of equity. These figures are based on Howard's observations in the course of consulting with various industries; the approach has received attention

from the decision and risk management community [Clemen and Reilly 2001, Kirkwood 1997, Soo Hoo 2000).

- Qualitatively: Management asks illustrative questions to elicit characteristics of the risk posture. Then, risk is expressed using a risk map, where the impact and likelihood of a given action are rated as low, medium or high. For example, a manager may ask, "What level of capital or earning is the organization willing to put at risk at a given a particular confidence level?"

5. Risk Management in Information Systems

Perhaps the most important reason for both businesses and consumers to refrain from establishing and participating in Internet-based information systems is the lack of trust and the potential for loss of assets and privacy caused by potential security breaches in such systems (Gordon 2002). A review of cases prosecuted by the Department of Justice, including the evaluation of damages and financial awards, shows a significant negative market reaction to information security breaches involving unauthorized access to confidential data, but no significant market reaction when the breach does not involve access to confidential data (Campbell 2003). This finding is consistent with the findings of the 2006 CSI/FBI survey, which suggests that among information security breaches, serious financial losses were related to the theft of proprietary information and unauthorized access (Gordon 2005).

The literature review also indicates that compromised firms, on average, lose approximately 2.1 percent of their market values within two days surrounding the compromise events (Cavusoglu 2002). This study suggests that smaller firms are penalized more than larger ones. However, initial investigations by other researchers indicate that, in some business sectors in the long term, stock prices rebound relatively quickly. Clearly, there are some market penalties for security breaches, and the literature indicates that Internet firms are penalized more than conventional firms, perhaps because of the former's dependence on the Internet to generate revenue.

Researchers have attempted many times to classify security threats; see, for example (Landwehr et al. 1993, Lipmann et al. 2000, Neumann 1989, Schneier 1996). The ISO standard 7498-2 (ISO 1989) lists five security control measures to combat these threats:

- Authentication,
- Access control,
- Data confidentiality,
- Data integrity, and
- Non-repudiation.

This classification is widely accepted among computer security experts. We believe that, although these classifications address the most important computer security threats, the proposed classification schemes have two disadvantages: they do not cover all threats, and they do not allow threats to be considered independently.

Software development projects can use a *risk exposure matrix* to organize and understand the risks facing them (Williams 1999). The matrix characterizes various possible project outcomes with respect to performance, support, cost, and schedule. Project managers or risk analysts offer a workshop in which participants score the various risk types and then relate them in a hierarchical interrelationship digraph. Next, each risk is matched with a selection of mitigation measures. Carnegie Mellon University's Software Engineering Institute (CMU) takes a more general approach to software risk (CMU 2006). Similarly, the National Institute of Technology (NIST) and International Standards Organization (ISO) recommend two general approaches for selection of control measures:

1. Baseline approach. The minimum level of security defined by an organization is selected for each type of information system. Then, baseline security is achieved by implementing a minimum set of control measures known as baseline control measures
2. Selection based on security concerns and threats. This approach requires more in-depth assessment for the selection of effective and suitable control measures. It provides support for

that selection by taking into account the high level view of security concerns (according to the importance of the asset) and likely threats.

In its guidelines on computer incident handling (Grance 2004) NIST also recommends the ISO approach and encourages organizations to create written guidelines for prioritizing incidents. According to NIST, prioritizing individual incidents, a critical step in the incident response process, can be based on the following:

- Criticality of the affected resources (e.g., public Web server, user workstation)
- Current and potential technical effect of the incident (e.g., root compromise, data destruction).

The likelihood of a potential vulnerability to be exploited by a given threat-source can be described as high, medium, or low (Stonebumer 2001):

- *High likelihood*. The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being penetrated are ineffective.
- *Medium likelihood*. The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
- *Low likelihood*. The threat-source lacks motivation or capability, or controls are in place to prevent (or at least significantly impede) the vulnerability from being exercised.

An extended version of this approach is used in the probability assessment of security incidents, as described in Farahmand et al. (2005). A different approach is presented by Camp and Wolfram (2004), which recommends a formal pricing mechanism for *externalities* to encourage organizations to respond to security threats and vulnerabilities. Such an approach would improve regulatory and market mechanisms by putting the burden of security costs on the information service provider. The Information Assurance Technical Framework Forum (IATF) of the National Security Agency (NSA) is also attempting to organize a framework for technical security countermeasures and information assurance solutions that

meet customers' needs and foster the development and use of solutions that are compatible with the framework (IATF 2006).

6. Risks to Procedural Fairness and Trust

Information systems business experts argue that organizations can address privacy and trust concerns and gain business advantage (for example, through customer recruitment or retention) by observing procedural fairness—that is, the perception by an individual that a particular activity in which he or she is a participant is conducted fairly (Culnan 1993, Lind and Tyler 1988, Milberg et al. 2000, Smith et al. 1996). In this sense, "fairness" means the Principles of Fair Information Practice suggested by a federal commission in 1973 that provides the basis for the U.S. federal privacy law enacted in 1974 [ware 1973]. The practices include:

1. Notice/Awareness. Consumers should be informed of an organization's information practices before asked to supply any personal information. The scope of the notice should include:
    - Who will collect the data
    - How the data will be collected
    - Whether supplying the data is mandatory or voluntary, and the consequences of refusal
    - To what uses the data will be put
    - Who might receive the data
    - How the data's confidentiality, integrity and quality will be protected
2. Choice/Consent. Presenting options about how the collected information may be used, including secondary uses.
3. Access/Participation. How an individual can access the data, not only to view information but also to contest its accuracy and completeness.

4. Integrity/Security. The data must be accurate and secure, with protection not only against loss but also against unauthorized access, modification, destruction or use.
5. Enforcement/Redress. The mechanisms available to enforce the principles and provide redress.

Procedural fairness is perceived as providing the consumer with a voice, and giving a consumer control over actual outcomes (Folger and Greenberg 1985, Lind and Tyler 1988). From this perspective, customers are assumed to be willing to disclose personal information and have that information used subsequently to create consumer profiles for business use when fair procedures such as these are in place to protect individual privacy. Studies indicate that individuals are less likely to be dissatisfied even with unfavorable outcomes if they believe that the procedures used to derive those outcomes are fair (Folger and Bies 1989, Greenberg 1987, Lind and Tyler 1988). Pavlou and Gefen (2005) explain psychological contract violation (PCV) as a buyer's perception of having being treated wrongly regarding the terms of an exchange agreement with an individual seller.

Moreover, studies on trust suggest that individuals are willing to disclose personal information in exchange for some economic or social benefit subject to the "privacy calculus," an assessment that their personal information will subsequently be used fairly and they will not suffer negative consequences (Milne and Gordon 1993, Stone and Stone 2003). For example, a survey of Internet users conducted by researchers at Georgia Institute of Technology (Georgia 1996) found that 78 percent of the survey participants would be willing to provide demographic information about themselves to the owner of a web site if "a statement was provided regarding how the information was used." Only 6 percent of the participants would not disclose demographic information under any circumstances. In general, individuals are less likely to perceive information collection procedures as privacy-invasive when

- Information is collected in the context of an existing relationship,
- They perceive that they have the ability to control future use of the information,
- The information collected or used is relevant to the transaction, and
- They believe the information will be used to draw reliable and valid inferences about them.

While the literature on customer service has not specifically addressed privacy, it has established a link between being treated fairly and customer satisfaction (Schneider and Bowen 1995).

7. Trust and Cyber Security

Many online organizations create trust by investing in cyber security practices and products. Table 1 describes the results of a survey of U.S. businesses where respondents describe their reasons for investing in cyber security. Although many are reacting to regulatory requirements or audits (the first and fourth categories, respectively), more than half (i.e., the remaining categories) derive from a need to trust their computer systems.

Table 1. Influences on Cyber Security Investment Strategy (Adapted from [88])

Categories of Influence	*Average Percentage Across Responding Organizations*
Regulatory requirement	30.1 %
Network history or information technology staff knowledge	18.9 %
Client requirement or request	16.2 %
Result of internal or external audit	12.4 %
Response to current events, such as media attention	8.2 %
Response to compromised internal security	7.3 %
Reaction to external mandate or request	5.0 %
Other	1.7 %

Indeed, the security of information systems is challenged by the proliferation of Internet-based applications, including electronic commerce and a variety of information brokering services. The growth in spending on cyber security occurs in a variety of areas, including software to detect viruses, firewalls, sophisticated encryption techniques, intrusion detection systems, automated data back up, and hardware devices (CERT 2006). Studies by the Computer Security Institute report that approximately 90 percent of respondent organizations detected computer security breaches with losses averaging over 2 million dollars per organization (Gordon 2005). In contrast, companies only spend 0.047 percent of their revenues on security (Geer and Soo Hoo 2003), suggesting that many firms are taking risks by not adequately investing in information security.

Why is this so? A literature review indicates that most cyber security research focuses on the technical defenses (e.g., encryption, access control, intrusion detection, and firewalls) associated with protecting information (Anderson 1972, Daniels 1999, Sandhu et al. 1999, Schneier 1996). However, until recently (with the advent of the five Workshops on the Economics of Information Security, WEIS), little comprehensive research addressed how organizations should:

- Assess the damages of past security incidents,
- Evaluate the risk of vulnerability to security incidents,
- Prepare for facing security incidents by selecting appropriate control, measures, given the resource constraints of finances, manpower, and software tools, and
- Train security personnel to better prepare for dealing with security incidents.

Limited data exist to describe the extent to which organizations invest in cyber security particularly to increase trust. The general cost of information systems security incidents is described in Anderson (2001), Butler (2002), Cohen (1991), Dobson (1994), Orlandi (1991), Tarr (1995) (See Pfleeger et al. (2006) for a discussion of available cyber security data). In 2007, the U.S. Bureau of Justice Statistics will reveal the results of the first large-scale, comprehensive survey of cyber security investment. Using a rigorous sample of 36,000 U.S. businesses, the data should provide benchmarks

about the number and type of cyber attacks, the nature and degree of investment in products and processes, and more (Office 2006).

Nevertheless, problems remain. For example, after a breach, often the damage is invisible, its extent delayed or unknown. Some researchers, such as Gordon and Loeb (2002), have suggested using return on investment techniques to determine an optimal level of cyber security investment, but others such as Willemson (2006) have argued against this approach. Other researchers, such as Rowe and Gallagher (2006), describe two distinct investment strategies: fixed cost and fixed security. In the first case, an organization determines how much money it can spend on cyber security, and then tries to maximize the amount of security it can get for that sum. In the second case, an organization determines how much security it needs, and then spends whatever sum is necessary to achieve that level of security. Similar perspectives can be taken with trust, where an organization either creates as much trust as it can for a given sum, or spends whatever is necessary to reach a given level of trust.

Kim and Benbasa (2003) organized key trust-related issues in Internet stores into four categories of personal information: product quality, price, customer service, and store presence. Based on a study of eBay's and Amazon's online auction marketplaces, Gefen and Pavlou (2006) show that the impact of trust on transaction intentions will increase as the buyer's perceived regulatory effectiveness increases from low to medium levels, but it will decrease as the buyer's perceived effectiveness increases from medium to high levels. They also show the perceived regulatory effectiveness of the online marketplace is hypothesized to reduce the impact of perceived risk on transaction intentions.

Farahmand et al. (2005) suggest that breaches of trust are considered to be the most serious cyber offenses. They conducted personal interviews with law enforcement agencies dealing with computer crime and with executives from variety of industries dealing with security issues. In addition, they did a literature review of cases prosecuted by the Department of Justice, including the evaluation of damages and financial awards. Consistent with the prior research Camp and Wolfram (2004) found a significant negative market reaction to information security breaches involving unauthorized access to confidential

data, but no significant market reaction when the breach does not involve access to confidential data. Surveys such as CSI/FBI Survey (Gordon 2005) reveal that, among information security breaches, respondents consider the most serious financial losses to be those related to theft of proprietary information. This finding is also consistent with computer cases recently prosecuted by the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. According to CCIPS, 91 percent of the cases prosecuted under the computer crime statute, 18 U.S.C. 1030, are those related to violation of information confidentiality. For example, in November 2001, two former Cisco Systems, Inc., accountants were sentenced to 34 months in prison for illegally issuing almost $8 million in Cisco stock to themselves: a clear breach of trust.

Thus, breaches involving unauthorized access to confidential information are quite different from attacks that do not involve access to confidential information. Once confidential information has been accessed in an unauthorized manner, the value of such a strategic asset may be permanently compromised. For example, a firm's customer list may be an important proprietary asset. Once this list has been accessed without authorization, others may be able to use the list for marketing and other purposes, permanently damaging the list's value to the firm that created it. When breaches do not involve unauthorized access to confidential information, the underlying assets generally relate to operations.

8. Trust and Risk in Cyberspace

The importance of confidentiality indicates that trust and risk are intertwined when organizations decide on cyber security investments. Pavlou (2003) integrates trust and risk as well as variables of the technology acceptance model into a research model. It is not often that firms have the luxury of making fixed security or fixed trust investments. Rather, managers ask their information technologists, "How much security can I get for my IT budget?" Thus, an organization's growing dependence on information technology, and particularly on online environments, carries with it a concomitant risk of adverse effects.

The role of economics is to help mitigate the risk. Viewed in this light, it may be more appropriate for organizations to perform risk-benefit rather than cost-benefit analysis, especially when trust is an essential characteristic of important relationships.

There is a rich literature on risk (see, for example Hollander and Mayo (1991)) that describes many aspects of risk that affect decision-making. For example, Starr (1969) derives several "laws of acceptable risk," including:

- The acceptability of risk is approximately proportional to the cube of the benefits.
- The public is willing to accept risk from voluntary activities (such as driving a car or opening an electronic attachment) at a level 1000 times greater than from involuntary activities (such as extreme weather events).
- The acceptable risk is inversely related to the number of people exposed to the risk.

Starr bases his work on historical record. However, Fischoff et al. (1978) point out that "what is accepted in the market may not accurately reflect the public's preferences." Indeed, some companies take greater risks in cyberspace or in financial markets, assuming that the cost of a breach or error is simply the cost of doing business. Moreover, many users of an online environment may not understand its technological underpinnings and relationships, so that "market behavior may not indicate what a reflective individual would decide after thoughtful and sensitive inquiry." Thus, rather than evaluate risk and trust based on preference revealed from past history, Fischoff et al. (1978) suggest using perceived and expressed preference, based on administration of questionnaires.

Fischoff et al. (1978) investigated perceptions of risk, and particularly ways to determine when a product is acceptably safe. Their findings are equally applicable to determining when a product or process is acceptably trustworthy. In this section, we describe their findings and discuss how they relate to online trust.

The participants in the Fischoff study were asked to rate an activity or technology on nine seven-point scales, each of which could influence risk perception (Lowrance 1976):

- Voluntariness
- Immediacy of effect
- Knowledge about the risk
- Control over the risk
- Novelty
- Chronic or catastrophic
- Degree of dread
- Severity of consequences

The researchers found that activities with the most dread and with certain severe consequences (in this case, certain fatality) were deemed to need the most risk reduction. In addition, if risk is adjusted to an acceptable level, then higher risks are tolerated for old, voluntary activities with well-known and immediate consequences. Finally, for any given benefit, greater risk was tolerated if it was voluntary, immediate, known precisely, controllable and familiar.

These results translate easily to a consideration of trust. The nine degrees of risk can be recast as characteristics of a trust relationship between actors A and B:

- Voluntariness: Does A choose to trust B (e.g. when providing credit card information online), or must A choose B (e.g. when employee A is directed by manager B to use a particular online service)
- Immediacy of effect: When does A's trust in B result in a clear effect?
- Knowledge about the risk: Does A know the risk of trusting B?
- Control over the risk: Can A control the conditions under which B is trusted?
- Novelty: Does A already know B and have an established trust relationship and history?
- Chronic or catastrophic: If B turns out not to be trustworthy, how many people are affected?

- Degree of dread: If B turns out not to be trustworthy, can A calmly deal with the consequences?
- Severity of consequences: If B turns out not to be trustworthy, are the results irreversible?

Thus, trust relationships involving the most dread and with certain severe consequences (from misplaced trust) may need the most risk reduction. We have seen that breaches of confidentiality are considered the most severe. So systems to engender or enforce trust online should focus first on protecting confidentiality. This is no mean feat, considering that online environments cross national boundaries, with each nation having different privacy statutes.

The Fischoff results suggest which online trust relationships will be the most comfortable. In addition, if trust involves risk at an acceptable level, then higher risks are tolerated for established trust relationships involved in voluntary activities with well-known and immediate consequences. Moreover, for a given level of trust, greater risk is tolerated if the trust relationship is voluntary, with results that are immediate, known precisely, controllable and familiar. Thus, the Fischoff results provide guidelines for the best ways to establish online trust relationships.

In turn, the Fischoff results suggest effective paths to economic gain. Since trust is an economic good that is clearly essential to online interactions, improved online trust relationships reduce risk and encourage more online economic transactions.

9. Conclusions

The main objective of this paper was to show that economic decision-making in online environments without consideration of trust and risk is not likely to be optimal. Arrow (1971) posits that even though it should be “rational economic behavior” to cheat or disregard trust, agents exhibiting trust and confidence are an essential part of a successful economy. He also recognizes that to improve efficiency, trust can be

enhanced via non-market controls, which can be endogenous (the inherent qualities of individuals) or exogenous (provided by third parties).

High trust results in lower cost, higher efficiency, minimal contracting, and a minimum of transaction-monitoring. Indeed, a high level of trust enables a high level of risk taking, because trust is the mirror image of risk: high trust suggests low perceived risks (Pauline 1999). For example, long term trading partner relationships can be sustained only via positive trust. However, the use of power among trading partners may affect them for a short period of time. Thus, acquiring and using power effectively and positively is necessary for success in organizations, at least for maintaining trading partner relationships, particularly online.

Guerra et al. (2003) suggest four strategies that meet the demands of information economy to enhance trust in online environments:

Identity establishment. Establish both the personal authentication of the consumer by the online supplier and trust in the identity and reputation of the supplier by the consumer.

Third-party certification. Reveal information about characteristics that cannot be otherwise observed by individuals.

Loss insurance. Limit the potential damage caused to a consumer in an online transaction

Legal frameworks. Reduce temptation by making illegal activities expensive, and use different regulatory and legal frameworks to address different trust concerns.

Recognizing the importance of trust and understanding the "dynamics of the system" that destroy trust has vast implications for how we approach risk management in the future. Slovic (1993) explains that early studies of risk perception demonstrated that the public's concerns could not be blamed simply on ignorance or irrationality. Instead, many of the public's reactions to risk could be attributed to a

sensitivity to technical, social, and psychological qualities of hazards that were not well-modeled in technical risk assessments (e.g., qualities such as uncertainty in risk assessments, perceived inequity in the distribution of risks and benefits, and aversion to being exposed to risks that were involuntary, not under one's control, or dreaded). The important role of socia1 values in risk perception and risk acceptance thus became apparent. There is a lot to learn from previous research on users' perceptions of risk of different technologies. However, we should acknowledge the active role of users in online environments that differentiates information technology from many other technologies. In online environments, users actually operate the technology, something that almost never happens in other situations, such as nuclear power (Sjöberg and Fromm 2001).

We stress the need for organizations to consider user perceptions of risk when establishing trust with their customers. To address this need, organizations should align users' perception with their organizational policies. Efforts should be made to develop a standardized approach to trust and risk across different domains to reduce the burden on consumers who seek to better understand and compare policies and practices across these organizations. This standardized approach will also aid organizations that engage in contractual sharing of consumer information, making it easier to assess risks across organizations and to monitor practices for compliance with contracts, policies and law.

It is important for individuals to observe that a particular activity in which they are participants is conducted fairly and addresses their privacy concerns. This observation also gives customers confidence in fair procedures and makes them more willing to disclose personal information—and to allow that information subsequently to be used to create consumer profiles for business use.

Thus, it is essential to monitor user perceptions. A promising approach to studying perceptions of hazards associated with technologies employs the psychometric paradigm, using psychophysical scaling and multivariate analysis techniques to produce quantitative representations or "cognitive maps" of risk attitudes and perceptions. The nine characteristics (e.g., immediacy of effect, newness, control, etc.) hypothesized by various authors to influence judgments of perceived and acceptable risk have been found

to be highly interrelated and can be effectively reduced to the two dimensions of dread and unknown risk. However, policy makers must observe that there is a difference between perceived risk and acceptable risk that indicates dissatisfaction with the way that market and regulatory mechanisms have balanced risks and benefits.

We posit that trust is an organizational and multidisciplinary issue. Without an organizational policy governing fair use of personal information, organizations face the risk that information used inappropriately by a single employee or by a single department can have negative consequences for the entire firm. In this regard, the United States Public Policy Committee of the ACM (USACM) advocates a proactive approach to privacy and trust policy by both government and private sector organizations, and recommends that organizations consider minimization, consent, openness, access, accuracy, security, and accountability in dealing with the personal information of online users Spafford (2006).

There are many practices and processes that can be implemented today to engender and promote these characteristics. Organizations can implement fair and trustworthy systems in a cost-effective way by using de-identified data, aggregated data, limited datasets, narrowly defined and fully audited searches. At the same time, we can work to develop new technologies to establish and protect trust while minimizing risk in online relationships and interactions.

References

Abdel-Rahman, M. S. et al. 2000. Peer Review Panel Report for the Fox Rive Human and Ecological Risk Assessments. Assoc. for Environmental Health and Sciences, Amherst, MA.

Aldrich, H. E., and C. Fiol, 1994. Fools Rush in? The Institutional Context of Industry Creation. *The Academy of Management Review*, 19(4), pp. 645-670.

Allen, W. D. 2000. Social Networks and Self-Employment. *Journal of Socio-Economics*, Vol.29, pp. 487-501.

Anderson, J. 1972. Computer Security Technology Planning Study. U.S. Air Force Electronic Systems

Division Tech. Rep., Oct. 1972, pp. 51-73.

Anderson, R. 2001. Why Information Security is Hard- An Economic Perspective. *17th Annual Computer Security Applications Conference*, Dec. 2001.

Annette, B. 1986. Trust and Antitrust. *Ethics*, 96, pp. 231-260.

Arrow, K. 1971. Essays in the Theory of Risk Bearing, North-Holland, Netherlands.

Baker, J. 1987. Trust and Rationality. *Pacific Philosophical Quarterly*, 1987, 68, pp. 1-13.

Baron, J. 1998. Trust: Beliefs and Morality in Avner Ben-Ner and Louis Putterman (eds.), *Economics, Values and Organization*, Cambridge University Press, Cambridge, UK.

Bartol N., N. Givans. 2001. Measuring the "Goodness" of Security. 2nd International System Security Engineering Association (ISSEA) Conference Proceedings, February 2001.

Butler, S. A. 2002. Security Attribute Evaluation Method: A Cost-BenefitApproach. *Proceedings of the* 24th International Conference on Software Engineering, ACM, May 2002, pp. 232-240.

Campbell, K., L. A. Gordon, M. P. Loeb, L. Zhou. 2003. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, Vol. 11, pp. 431-448.

Camp, L. J., C. Wolfram. 2004. Pricing Security – A Market in Vulnerabilities. in Camp, L. Jean, and Stephen Lewis (Eds.), *Advances in Information Security; Economics of Information Security*, Kluwer Academic Publications, pp. 17-34.

Cavusoglu, H., B. Mishra, S. Raghunthan. *The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers*. University of Texas at Dallas, 2002.

CERT 2006, http://www.cert.org

Charnley, G. 2000. Democratic Science: Enhancing the Role of Science in Stakeholder-Based Risk Management Decision-Making. Washington, DC: Health Risk Strategies.

Clemen, R. T., T. Reilly. 2001. Making Hard Decisions. Duxbury.

Cohen, F. 1991. A Cost Analysis of Typical Computer Viruses and Defenses. *Computers & Security*, Vol. 10, pp. 239-250.

CSO. 2004, The Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management- Integrated Framework.

Culnan, M. J. 1993. How Did they get My Name? *MIS Quarterly*, pp. 341-363.

Culnan, M. J. 1999. Information Privacy Concerns, Procedural, Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, Vol. 10, No. 1, Jan-Feb 1999, pp. 104-115.

Daniels, T. E., E. H. Spafford. 1999. Identification of Host Audit to Detect Attacks on Low-level IP, *Journal of Computer Security*, Sec. 7- 1, pp. 3-35.

Deelmann, T., and P. Loos. 2002. Trust Economy. *Eighth Americas Conference on Information Systems*, pp. 2213-2221.

Deephouse, D. L., 1996. Does Isomorphism Legitimate?. *Academy of Management Journal*, 39(4).

Denning, D. 1987. An Intrusion-detection Based Model. *IEEE Transaction on Software Engineering*, Vol. 13, No. 2, Feb. 1987, pp. 222-226.

Dobson, J. 1994. Messages, Communication, Information Security and Value. *Proceeding of the New Security Paradigms Workshop*, IEEE, Aug. 1994, pp. 10-18.

Earle ,T. C. 2004. Thinking Aloud about Trust: A Protocol Analysis of Trust in Risk Management.

Elliott, M. R., Y. Wang, R. A. Lowe., P. R. Kleindorfer, P. 2004. Environmental Justice: Frequency and Severity of U.S. Chemical Industry Accidents and the Socio-economic Status of Surrounding Communities. *Jrl. Epidemiology and Community Health*, 58(1), 24-30.

Farahmand, F., S. B. Navathe, G. P. Sharp, P. H. Enslow. 2003. Managing Vulnerabilities of Information Systems to Security Incidents. *ACM ICEC 2003*, Pittsburgh, Sept. 2003.

Farahmand, F., S. B. Navathe, G. P. Sharp, P. H. Enslow. 2005. A Management Perspective on Risk of Security Threats to Information Systems. *Journal of Information Technology & Management*, Springer Publications, Apr. 2005, Vol. 6, Numbers 2-3, pp. 203-225.

Farahmand, F., S. B. Navathe, G. P. Sharp, P. H. Enslow. 2005. Assessing Damages of Information Security Incidents and Selecting Control Measures, a Case Study Approach. *Proceedings of the Workshop on the Economics of Information Security*, Boston, Massachusetts.

Fischoff, B. et al. 1978. How Safe Is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits? *Policy Sciences* 9(2), April 1978, pp. 127-152.

Folger, R. and J. Greenberg. 1985. *Procedural Justice: An Interpretive Analysis of Personnel Systems* in Kendrith M, Rowland and Gerald R, Ferris *Research in Personnel and Human Resources Management,* 1985, Vol 3, Greenwich, CT: JAI Press, 141-183

Folger, R., R. J. Bies, R. 1989. Managerial Responsibilities and Procedural Justice. *Employee Responsibilities and Rights Journal*, 2, pp. 79-90,

Gambetta, D. 1988. *Trust: Making or Breaking Cooperative Relations*, Basil Blackwell, Oxford, UK.

Geer, D., K. J. Soo Hoo, K., A. Jaquith. 2003. Information Security: Why the Future Belongs to Quants. *IEEE Security and Privacy*, pp. 32-40.

Gefen, D., P., P. A. Pavlou. 2006. The Modeling Role of Perceived regulatory Effectiveness of the Online Marketplaceson the Role of Trust and Risk Transaction Intensions. Proceeding of the 27th ICIS Conference, Milwaukee, WI.

Georgia 1996, Georgia Tech Research Corporation, Fifth WWW User Survey.

Gordon L. A., M. P. Loeb. 2002. Return on Information Security Investments. *Strategic Finance*, Nov. 2002.

Gordon, L. A. et. al. 2005. CSI/FBI *Computer Crime and Security Survey.,* Computer Security Institute.

Grance, T., K. Kent, B. Kim. 2004. *Computer Security Incident Handling Guide*, NIST, SP 800-61, Jan. 2004.

Greenberg, J. A Taxonomy of Organizational Justice Theories, *Academy of Management Review*, 1987, 12, 1, pp. 9-22.

Guerra G. A. et al. 2003. Economics of Trust in the Information Economy, Oxford Internet Institute,

Research Report No. 1, Apr. 2003.

Gui, B. 2005a. From Transactions to Encounters: The Joint Generation of Relational Goods and Conventional Values, pp. 23-51.

Gui, Benedetto, R. Sugden (eds.), 2005b. *Economics and Social Interaction: Accounting for Interpersonal Relations,* Cambridge University Press, Cambridge, UK.

Gui, B. Sugden, R. 2005c. Why Interpersonal Relations Matter for Economics, in Gui and Sugden 2005a, pp. 1-22.

Henley, E.J., H. Kumanota. 1981. *Probabilistic Risk Assessment, Reliability Engineering, Design, and Analysis*, IEEE Press, New York.

Horsburgh, H. J. N., 1960. "The Ethics of Trust," *Philosophical Quarterly*, 10, pp. 343-354.

Howard, R. A. 1988. *Decision Analysis: Practice and Promise*. *Management Science*, 34, pp. 679-695.

IATF 2006. http://www.iatf.net/

IRM. 2006. *A Risk Management Standard*, Institute for Risk Management, London, UK

ISO. 1989. Information Processing Systems- Open Systems Interconnection-Basic Reference Model, Part 2: Security Architecture. *ISO 7498-2.*

Jensen, C., C. Potts. 2004. Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. P*roceedings of the ACM SIGCHI conference on Human factors in computing systems,* Apr. 2004, pp. 471-478.

Jones, K. 1996. Trust as an Affective Attitude. *Ethics,* 107, pp. 4-25.

Jones, G.R., J. M. George. 1998. The Experience and Evolution of Trust: Implications for Cooperation and Teamwork. *The Academy of Management Review*, 23(3), pp. 531.

Kapur, K. C. 1982. *Reliability and Maintainability*, in Salvendy, G. (Ed.), Handbook of Industrial Engineering, John Wiley & Sons, New York, 1921-1955.

Keeney, R. L., H. Raiffa. 1976. Decisions with Multiple Objectives: Preferences and Value Tradeoffs. John Wiley & Sons.

Kim, D., Benbasat, I. 2003. Trust-Related Arguments in Internet Stores: A Framework for Evaluation. J. Electron. Commerce Res. 4 (2): pp. 49-64.

Kirkwood, C. W. 1997. Strategic Decision Making, Duxbury.

Kleindorfer, P. R., M. R. Elliott, Y. Wang, R. Lowe. 2004. A.Drivers of accident preparedness and safety: evidence from the RMP rule. *Journal of Hazardous Materials*, Vol. 115, 9-16.

KPMG. 2006. U.S. *Project Management Reference Manual*. KPMG U.S. Executive Office, Montvale, NJ.

Kunreuther, H. 2001. *Risk Analysis and Risk Management in an Uncertain World*. *Risk Analysis*, 02-08, Wharton School Center for Financial Institutions, University of Pennsylvania, 25 pages.

Landwehr, C. E., et al. 1993. *A Taxonomy of Computer Program Security Flaws with Examples*. Naval Research Laboratory, Nov. 1993.

Lind, E, A., T. R. Tyler. 1988. *The Social Psychology of Procedural Justice,* New York: Plenum Press.

Lipmann, R., et al. 2000 The 1999 DARPA off-line Intrusion Detection Evaluation. *Computer Networks*, Vol. 34, pp. 579-595.

Lowrance, W. W. 1976. *Of Acceptable Risk,* William Kaufman, Inc., Los Altos, California.

Hollander, D., R. Mayo. 1991. Acceptable Evidence: Science and Values in Risk Management. Oxford University Press.

McAllister, D. J. 1995. Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. *Academy of Management Journal*, 38(1), Briarcliff Manor, pg. 24, 36 pages.

McCarthy, M. P., T. P. Flynn. 2004. Risk from the CEO and Broad Perspective. KPMG & McGraw-Hill.

Michel-Kerjan, Erwann. 2002. 'Risques catastrophiques et reseaux vitaux: de nouvelles vulnerabilites," (Catastrophic risks and vital networks: new vulnerabilities) Wharton School Center for Financial Institutions, University of Pennsylvania, Flux – International Scientific Quarterly on Networks and Territories, 20 pages.

Milberg, S. J., H. J. Smith, S. J. Burke. 2000. Information Privacy: Corporate Management and National

Regulation, *Organization Science*, Vol. 11, No. 1, Jan-Feb 2000, pp. 35-57.

Milne, G. R., M. E. Gordon. 1993. Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework. *Journal of Public Policy & Marketing,* 12, 2, Fall 1993, pp.206-215.

Muermann, A., O. Ulku. 2002. The Near Miss of Operational Risk. *The Journal of Risk Finance*, Vol. 4, No. 1, Fall 2002.

Neumann, P. G., D. B. Parker. 1989. A Summary of Computer Misuse Techniques. *Proceedings of the 12th National Computer Security Conference*, Oct. 1989, pp. 396-407.

Office 2006. Office of Justice Programs, Department of Justice Statistics. National Computer Security Survey Announced. Press Release, February 9, 2006 www.ojp.usdoj.gov/bjs/survey/ncss/ncss.htm

Orlandi, E. 1991. The Cost of Security. *Proceeding of the 25th Annual IEEE International Carnahan Conference on Security Technology*, Oct. 1991, pp. 192 –196.

Pavlou, P. A. 2003. Consumer Acceptance of Electronic Commerce- Integrating trust and Risk, with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7(3): 69-103.

Pavlou, P. A., D. Gefen. 2005. Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role. *Information Systems Research*, 16(4): 272-299.

Pelligra, V. 2005. Under Trusting Eyes: The Responsive Nature of Trust. (in Gui and Sugden), pp. 105-124.

Pettit, P. 1995. The Cunning of Trust. *Philosophy and Public Affairs*, 24(3), pp. 202-225.

Pfleeger, S. L., R. Rachel, J. Horwitz, A. Balakrishnan, 2006. Investing in Cyber Security: The Path to Good Practice. *Cutter IT Journal*, 19(1), January 2006.

Pfleeger, C. P., S. L. Pfleeger, 2007. *Security in Computing*, Fourth Edition, Prentice Hall.

Pfleeger, S. L., M. Libicki, M. Webber. 2007. Trusting Business: Suggestive Findings About Cyber Security. *IEEE Security and Privacy*, May/June 2007, to appear.

Rabin, M. 1993. Incorporating Fairness In to Game Theory and Economics. *American Economic Review*,

1993, 83(5), pp. 1281-1302.

Raiffa, H., R. Schlaifer. 1961. *Applied Statistical Decision Theory*. Harvard Univ. Business Press.

Pauline R. 1999. Risks in Low Trust among Trading Partners in Electronic Commerce. *Computers & Security*, 18 , pp. 587-592.

Rowe, B. R., M. P. Gallagher. 2006. Private Sector Cyber Security Investment Strategies: An Empirical Analysis, *Proceedings of the Fifth Annual Workshop on the Economics of Information Security*, June 2006, Cambridge, UK. Available at http://weis2006.econinfosec.org/docs/18.pdf

Sandhu, R. S., E. J. Coyne, and C. E. Youman. 1999. Role-based Administration of Rules. *ACM Transactions of Information Systems*, Sec. 1, 2, Feb. 1999, pp. 105-135.

Schneier, B. 2002. No, We Don't Spend Enough. *Proceedings of the Workshop on Economics of Information Security*, May 2002.

Schneider, B., D. E. Bowen. 1995. *Winning the Service Game,* Boston, MA: Harvard Business School Press.

Schneier, B.1996. *Applied Cryptography.* Wiley, New York.

Shtub, A.; Bard, J.; and Globerson, S. Project Management Engineering, Technology, and Implementation, Prentice-Hall, Englewood Cliffs, NJ, 1994.

Sjöberg, L., J. Fromm. 2001. Information Technology Risks as Seen by the Public. *Risk Analysis*, Vol 21, No. 3, pp. 427-441.

Slovic, P. 1993. Perceived Risk, Trust, and Democracy. *Risk Analysis*, Vol. 13, No. 6, pp. 675-682.

Smith, H., S. J. Milberg, S. J. Burke. 1996. Information Privacy: Measuring Individual's Concerns about Organizational Practices. *MIS Quarterly*, Jun 1996, pp.167-195.

Smyth, A.W. *et al.* 2003. Probabilistic Benefit-Cost Analysis for Earthquake Damage Mitigation: Evaluating Measures for Apartment Houses in Turkey. *EERI Earthquake Spectra,* 20-1, pp.171-203.

Soo Hoo, K. J. 2000. How Much is enough? A Risk management Approach to Computer Security, Ph.D.

Dissertation, Stanford University, Advisor: Seymour E. Goodman.

Spafford, E. H. 2006. Editor & Chair, http://www.acm.org/usacm/Issues/Privacy.htm.

Starr, C. 1969. Social Benefit Versus Technological Risk. *Science*, 165, pp. 1232-1238.

Stone, E. F., D. L. Stone. 2003. Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms. in K, M, Rowland and G, R, Ferris (Eds), *Research in Personnel and Human Resources Management,* Vol, 8, Greenwich, CT: JAI Press, 349-411.

Stonebumer, G., A. Goguen, A. Feringa. 2001. Risk Management Guide for Information Technology Systems. *NIST Special Publications 800-30*.

Stufflebeam, W. H., A. I. Anton, Q. He, N. Jain. 2004. Specifying Privacy Policies with P3P and EPAL: Lessons Learned. *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, pp. 35-36.

Tarr, C.J. 1995. Cost Effective Perimeter Security, Security and Detection. *European Convention on Security and Detection*, pp. 183-187.

Topa, G. 2001. Social Interactions, Local Spillovers and Unemployment. *Review of Economic Studies*, 68(2), pp. 261-295.

Ware, Willis et al. 1973. *Records, Computers and the Rights of Citizens,* Department of Health, Education and Welfare, US Government Printing Office.

Webster's Third New International Dictionary. 1986. Merriam-Webster Inc.

Willemson, J. 2006. On the Gordon and Loeb Model for Information Security Investment. *Proceedings of the Workshop on the Economics of Information Security*, Cambridge, UK, June 2006.

Williams, R. C., G. J. Pandelios, S. G. Behrens. 1999. *Software Risk Evaluation (SRE) Method Description (Version 2.0)*, CMU/SEI-99-TR-029, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA.

Zak, P.J., S. Knack, S. 2001. Trust and Growth, *Economic Journal*, 111, pp. 295-321.