Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2008 Proceedings

International Conference on Information Systems (ICIS)

1-1-2008

Incentives and Perceptions of Information Security Risks

Fariborz Farahmand
Purdue University, fariborz@purdue.edu

Mikhail Atallah
Purdue University, mja@cs.purdue.edu

Benn Konsynski
Emory University, Benn_Konsynski@bus.emory.edu

Follow this and additional works at: http://aisel.aisnet.org/icis2008

Recommended Citation
Farahmand, Fariborz; Atallah, Mikhail; and Konsynski, Benn, "Incentives and Perceptions of Information Security Risks" (2008). *ICIS 2008 Proceedings*. Paper 25.
http://aisel.aisnet.org/icis2008/25

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

www.manaraa.com

Incentives and Perceptions of Information Security Risks

Incitations et Perceptions des Risques pour la Sécurité de l'Information

Fariborz Farahmand
Center for Education and Research in Information Assurance and Security
Purdue University
e-mail: fariborz@purdue.edu

Mikhail Atallah
Center for Education and Research in Information Assurance and Security
Purdue University
e-mail:mja@cs.purdue.edu

Benn Konsynski
Goizueta Business School
Emory University
e-mail: Benn_Konsynski@bus.emory.edu

Abstract

Technologies and procedures for effectively securing cyberspace exist, but are largely under-deployed. One reason for this is that organizational - reward systems lack the proper incentives for decision-maker allocation of resources. We identify characteristics of differing stakeholder perceptions of security and privacy risks and integrate them in a decision making framework. We significantly revise the Fischhoff and Slovic model of risk perceptions --- introducing ordinal scales to the identified characteristics of risk perceptions, and incorporating the dynamics of perception by including the important and neglected time element. Over twelve months, we reviewed and verified the model with thirty five senior information security executives from industrial and governmental organizations. We present a methodology for identification of perverse incentives---situations where the interests of a manager or employee are not aligned with those of the organization; and how the policies and reward system may be modified to correct the mis-alignment.

Keywords: Incentives, information security, risk, perceptions, decision making

Résumé

L'une des raisons pour lesquelles les technologies pour la sécurité de l'information sont sous-déployées, est que les systèmes de récompense n'incitent pas les décisionnaires à une telle répartition de ressources, même quand l'intérêt de l'organisation l'exige. Cet article présente une méthodologie pour identifier de telles situations, et pour les corriger en alignant la motivation des décisionnaires avec l'intérêt de l'organisation.

www.manaraa.com

Introduction

Most research being carried out today in information security focuses on developing new security technologies (Anderson 2001, Varian 2000). At the same time, much of the technology is not being effectively utilized due to the problems that are endemic to the human dimension. Questions about why technologies are not being effectively implemented are critical to insuring that the best technology is meeting its intended purpose (Straub et al. 2008). Adoption and employment of critical technologies are often neglected or delayed as a result of fears or assumptions of risk to operations or exposure of reputation or brand. More recently (with the advent of the six Workshop on the Economics of Information Security, WEIS), systematic comprehensive research is increasingly addressing how organizations should:

- Assess the damages of past security incidents,
- Evaluate the risk of vulnerability to security incidents and the effectiveness of security technologies, and
- Quantify perceptions of risk by different stakeholders and incentives for the alignment of those perceptions.

Slovic (1987) argues that while technologically sophisticated analysts employ risk assessment to evaluate hazards, the majority of citizens rely on "institutive risk judgments," typically called risk perceptions. Anderson (2008) defines incentive as "the motive that people guarding and maintaining the system have to do their job properly, and also motive that the attackers have to try to defeat your policy". He identifies incentive along with policy, mechanism, and assurance as four required elements of security engineering analysis.

This research integrates perceptions of risk, benefit, and incentives in a framework within which a methodology is developed to align stakeholder perceptions of information security risks. In this research we use the theoretical foundation on perception of risk built by Baruch Fischhoff, Paul Slovic, and on behavioral economics by Daniel Kahneman and Amos Tversky who jointly won the Nobel Prize in economics in 2002 for launching this field. This paper, seeks to shed light on decision making in information security, more specifically, on perceptions of risk and incentives that influence the decision processes.

This paper will explore the following research questions:

1. What are the constructs of perceived information security risks, and the perceived benefits of addressing those risks?
2. How to identify and to re-align perverse incentives by different stakeholders?

We first provide a background on information security and economic incentives, risk compensation, and present some real world findings on stakeholder perceptions of risk. Next, we a present a literature review on the construction of preference, perceived benefit, and the inverse relationship between perceived risk and benefit. We present a framework for consideration of adequate incentives to align stakeholder perceptions, real risk considerations and appropriate allocation of rights and authorities. Then, we introduce a methodology for identifying perverse incentives, whose influence in other domains was documented in the economics literature -- see, e.g., Kerr (1975), Gibbons (1998), Lazear (2000), Stone and George (1997). We define consequences and understating as the two main characteristics of information security risks and by considering security as a process, and not as an object, we include the time element in our model and acknowledge the dynamics of perception -- a significant difference between our model and the model originally presented by Fishhoff and Slovic. Our model has been reviewed and verified with thirty five senior information security executives from industry and governmental organizations in one-on-one meetings in the past twelve months. We conclude our paper with a discussion of our results and implications for senior management.

Background

Information Security and Economic Incentives. The economics of information security has recently become a thriving and fast moving area, and incentives of organizations--as a whole-- to invest on information security and users to pay for security has been studied by several researchers. For example, Anderson and Moore (2006) found that incentives are becoming as important as technical design in achieving dependability. Loch et al. (1992) explain that employees and internal organizational procedures could be a greater threat than competitors. Odlyzko (2003)

www.manaraa.com

argues that what really motivates commercial organizations (even though they often do not realize it clearly themselves) is the growing incentive to price discriminate, coupled with the increasing ability to do so. Gordon (2007) argues that the most powerful incentive for an organization in the private sector to invest in cybersecurity activities is the motivation to increase the organization's value to its owners. Gordon and Loeb (2002) also suggested using return on investment techniques to determine an optimal level of cyber security investment, but others such as Willemson (2006) have argued that this traditional accounting approach is flawed. Farahmand et al. (2005) argue that a trade-off exists between the amount a firm should invest to protect against possible security breaches and the amount it should spend on cyber-risk insurance. Wash and MacKie-Mason (2007) designed incentive-centered design tools to help induce the desired behavior in users. Dynes et al. (2008) conclude that if the government is concerned about risks that are not concerns of individual firms, and endogenous economic forces are not present, then the government will have to address these risks in other ways.

Risk Compensation. Risk compensation theory is sometimes referred to as risk homeostasis or behavioral adaptation. It is the idea that after safety measures have been introduced, the level of risk is re-asserted at the level with which the subject was originally content (Stewart 2004). In the field of insurance the idea of risk compensation is known as ''moral hazard''. When someone is insured they often compensate by taking greater risks than they would ordinarily do, because they know that their insurance protects them financially. The insurance company may therefore receive more claims than their models predict. From a clinical perspective, fire insurance actually provides an incentive to commit arson if the payoff is greater than the value of the property. Most police investigations into arson are the result of leads from suspicious insurance adjusters. Stewart (2004) explains that if we look at the way that companies view information security we can see that risk compensation theory predicts many of their actions. A security incident tends to spur an organization to attempt to increase security, but then the enthusiasm for security within the organization tends to wane over time as the incident recedes in the organization's collective memory and the acceptable level of risk is reset at the original value. Because security professionals live and breathe security, their goal for the level of acceptable risk within a company usually does not match the company's perception of the acceptable level of risk. In its worst stages, this affliction can result in a state of deadlock between the internal security group and the business.

Variance in Stakeholder Perception of Risk. A key factor in the alignment of security and privacy risk initiatives with the strategic objectives of the enterprise is the considerable variance in the perceptions of level of threat and ownership of the risk responsibility by key managerial stakeholders in the enterprise. Recognition of these differences is important to effective investment in security measures that align with enterprise strategic objectives.

In the course of a 12-month study in 2005, Ernst & Young explored in detail the views of 700 senior decision makers on risk and risk management from three different stakeholder groups: investors, Executive Management and independent Board Members (Ernst & Young 2005). This study underscored the difference of perspective of different stakeholders on a variety of issues and the factors that influence their decisions. For example, on the issue of risk ownership, Board Members were most likely to identify themselves in this role (40%), followed by the CEO (21%). Conversely, Executive Management was most likely to identify the CEO (30%), followed by the Board as a whole (21%). Investors were less definitive, but lean towards recognizing the CEO as the ultimate owner of risk. The findings of this study also underscore the need for a logical and coordinated process that aligns an organization's risk management programs with its key business drivers and initiatives.

Elements in the Construct of Preference and Perceived Benefit

> *A bank in New York had a Chief Information Security Officer. This CISO wanted to invest in identity management. The system involved cost real money. The CISO got the money by asking what is essentially a risk aversion question: "This investment is worth it if the reputation capital of the firm is at least as much as one basis point of our market cap" (basis point = .01%). No officer of that bank was willing to bet the reputation of the firm as being worth less than .01% of the market value of the firm, and so the CISO got his identity management system (Geer 2007).*

www.manaraa.com

What are the constructs of preferences and incentives? What factors, internal or external, influence senior management's preferences and incentives and how do these factors affect their choice of construction methods? One of the main themes that has emerged from behavioral decision research during the past three decades is the view that people's preferences and incentives are often constructed in the process of elicitation. The following is an overview some of this research that applies to our research.

The Relative Importance of Probabilities in Risk Taking Plays a Significant Role in Effective Response. Slovic and Lichtenstein (1968) argue that the decision makers are guided by certain beliefs, which combine with strategies designed to make their task less complex. Such a strategy has two parts. First, gambles are classified as either attractive or unattractive. Then, the degree of attractiveness is quantified. This is proceeded by the decision maker--during bidding--as a crude adjustment of "amount to win" if the bet is attractive, or "amount to lose" if the bet is unattractive.

Choice and Matching Issues Arise in the Consideration of Security Risk Management. Tversky et al. (1988) frame real-world decisions either as a direct choice (e.g., should I buy the used car at this price?) or as a pricing decision (e.g., what is the most I should pay for that used car?). They suggest that the answers to the two questions are likely to diverge. For example, consider a medical decision problem where the primary dimension is the probability of survival and the secondary dimension is the cost associated with treatment or diagnosis. People are likely to choose the option that offers the higher probability of survival with relatively little concern for cost. When asked to price a marginal increase in the probability of survival, however, people are expected to appear less generous. The choice-matching discrepancy may also arise in resource allocation and budgeting decisions.

Schkade and Johnson (1989) find that choice compared with judgment, subjects take much less time, use different patterns of information search, and often employ strategies that make comparisons between two alternatives. In contrast, in the judgment modes, pricing and rating, subjects often use a strategy focused on the response scale in which a starting point is selected and then adjusted to arrive at response. Consistent with Tversky et al. (1988), they find systematic relationship between detailed process measures of such mechanisms and the frequency of reversals--anchoring and adjustment activity and differential attention to probabilities as the most indicators.

Inverse Relationship between Perceived Risk and Benefit. Kahneman et al. (1999) argue that people are better described as having attitudes than preferences—perhaps in every domain, but certainly in the domain of public concerns. Payne et al. (1992) claim that people do not have preferences, in the sense in which that term is used in economic theory. March and Shapira (1986) conclude not only that managers fail to follow the canons of decision theory, but also that the ways they think about risk are not easily fit into classical theoretical conceptions of risk.

Alhakami and Slovic (1994) found an inverse relationship between perceived risk and benefit that is indicative of a confounding of risk and benefit in people's mind. They argue that this confounding is linked to a person's overall evaluation of an activity or technology. They also argue that people operate under a strong need for consistency among their beliefs and attitudes. When people view an activity or technology as good, pressure toward consistency would lead them to judge its benefits as high and its risk as low, and vice versa for activities seen as bad. They also argue that the inverse relationship between perceived risk and perceived benefit of an activity is linked to the strength of positive or negative affect associated with that activity—the higher the perceived benefit, the lower the perceived risk, and vice versa. Finucane et al. (2000) suggest that the inverse relationship between perceived risk and benefit occurs because people rely on affect when judging the risk and benefit of specific hazards.

Slovic et al. (2007) defined affect as the specific quality of goodness or badness and explained that people use an affect heuristic to make judgments. That is representations of objects and events in people's minds are tagged to varying degrees with affect. In the process of making a judgment or decision, people consult or refer to an "affect pool" containing all the positive and negative tags consciously or unconsciously associated with the representations. Using an overall, readily available affective impression can be far easier than weighing the pros and cons or retrieving from memory many relevant examples, especially when the required judgment or decision is complex or mental resources are limited. This characterization of a mental short-cut leads to labeling the use of affect a "heuristic".

The affect heuristic also predicts that using time pressure to reduce the opportunity for analytic deliberation should enhance the inverse relationship between perceived benefits and risks. Finucane et al. (2000) showed that the inverse relationship between perceived risks and benefits increased greatly under time pressure as predicted. This is consistent with Zajonc's findings (1980) that affect influences judgment directly and is not simply a response to a prior analytic evaluation.

www.manaraa.com

It is incumbent on the enterprise security assessment to establish fair measurement of risk and benefit to inform the balance and tension that might otherwise cloud a security investment decision. Each stakeholder perception of exposure contributes to the assessment of risk in decisions of needed action and investment.

Perceptions Play no Small Role in the Organization Response to Information Privacy and Security Risk. The role of perception on information security risks has been studied by several researchers. Moores and Dhillon (2003) explain that with each new case of online fraud, the perception by consumers will continue to be that Internet thieves lurk in the shadows of cyberspace, widening the trust gap and constraining the legitimate commerce being carried out online. Goodhue and Straub (1991), and Straub and Welke (1998) argue that managerial concern about the organization's security is a function of: (1) risk inherent in the industry, (2) the extent of the effort already taken to control these risks, and (3) individual factors such as awareness of previous system violations, background in systems work, etc. Diamond (1988) explains that framing effects may act differentially according to the form in which they are presented. Graphic presentations are more apt to induce framing than tabular presentations. Kim and Prabhakar (2000) argue that trust in the electronic channel and perceived risks of e-commerce are the major determinants of the adoption behavior. Using economic modeling and computer simulation approaches, Hu et al. (2001) study the effect of traders' perceived risk on the adoption of online escrow service. Taylor (2006) finds that many of management's taken-for-granted assumptions about information security within their organization are inaccurate. He suggests that by increasing management's awareness of these risks, they will take precautions to eliminate this behavior to ensure that the organization's information is better secured. Based on a study of eBay's and Amazon's online auction marketplaces, Gefen and Pavlou (2006) show that trust's effect on transaction intentions will increase as the buyer's perceived regulatory effectiveness increases from low to medium levels, but will decrease as the buyer's perceived effectiveness increases from medium to high levels.

Seeking Alignment of Perceptions, Risks, and Incentives

> *The trouble is that most people think the question (How Safe is Safe Enough?) deserves an answer. Most people do not think in terms of comparative analyses of alternatives; they do not think in terms of value tradeoffs; they do not think in terms of uncertainties; they do not think about how one policy choice may set up a dynamic sequence of adjustments and that indirect effects may far outweigh immediate direct effects (Raiffa 1979).*

How then might we employ incentives to influence the decision processes of stakeholders to serve the nature of the risks and the interests of the organization? It is the nexus of the controls on decision rights and incentives to appropriately manage risks that are at the heart of our inquiries. We consider a framework for consideration of adequate incentives to align stakeholder perceptions, real risk considerations and appropriate allocation of rights and authorities.

Let X be an agent, in an organization O, who makes decisions that impact the security of information in O. For example, X may decide the amount of expenditures on information security (with other agents deciding how to spend that budget), or X may be provided a fixed budget for information security and must decide how to allocate it (i.e., which technologies to deploy, personnel to hire, etc). Each decision D that X makes, has different impact on X and O; some of these impacts are certain to occur whereas others depend on how the future unfolds (e.g., whether O suffers a serious break-in and the amount of loss resulting from it). Examples of the decisions by X (and some possible consequences) are:

A. Manager X can decide to invest (resp., not to invest) on better information security, and the unit that X manages looks less profitable by the amount spent. The organizational reward system ties X's bonus to the profitability of the unit that X manages.

B. X decides to recommend and request the deployment of an intrusion detection system, as a result of which the workload of Y (possibly Y=X) increases because of having to maintain the system and handle many false intrusion alarms.

www.manaraa.com

C. X decides to under-spend in (or under-deploy) security technologies, and a serious break-in occurs causing O to suffer considerable damage to its reputation from the newspaper headlines and from lawsuits by customers of O whose private data was compromised.

D. X decides to considerably invest in (or deploy) security technologies, and no break-in occurs.

We propose an approach that consists of carrying out a detailed analysis of the incentives of each entity X in O and identifying all the cases where the incentives of X are not aligned with those of O. This is done as a first step in modifying the organizational incentives system so that the incentives of every X become aligned with those of the organization. Before we do so, we give a few simple examples that illustrate the role of incentives.

Example 1: Under-Investing in Security as a Winning Proposition

Consider the situation where the above Case A applies, with X being a CEO. Were a serious security breach to occur, it is Chief Information Security Officer (CISO) who bears the brunt of the blame (e.g., a drastically lower bonus, or even a job loss). The extreme event of a devastating breach that puts O of out of business is unlikely – most breaches result in embarrassment and expensive (but typically manageable) lawsuits. If such an "expensive but manageable" breach were to occur, O would suffer considerable loss but it is Y not X who would get fired. But the more likely future is that no serious security breach occurs, in which case the unit managed by X is more profitable and X gets a higher bonus. This is a case of a perverse incentive – X is not incentivized to act in the best interests of the organization O: Under-investment in security is a likely winner for X even if O is (on average) worse off as a result. Y, on the other hand, is well incentivized to make the best use of the limited budget and resources allocated to information security by X. But if resources are inadequate, Case C may well occur and cost both O and Y dearly. This is not a hypothetical situation, as most serious security breaches leave the CEO in the job but result in the firing or the "voluntary departure to pursue other interests" of the CISO.

Example 2: Investing in Security as a Losing Proposition

Consider the situation where the above Case D applies. How does X claim credit for what did not occur? Someone may say "The company B on the third floor did not spend the $1M that O spent on information security, and B did not suffer a break-in either." Spending on security and achieving it is still damaging to X: It lowers the bonus because of the decreased profit, and it is hard to show a return on the investment by arguing that a headline-making security breach may have occurred otherwise. One way to properly incentivize X is to change the bonus reward policy so that it includes a positive reward if no serious security breach occurs, a reward larger than the negative effect of security expenditures on the profitability of the unit managed by X. Note that the cost of the deployment of security technologies and procedures is typically lower than the dollar amounts actually spent, because of the lower insurance premiums that result (the lower premiums are not enough to offset the expenditure but they must be subtracted from it in any cost-benefit analysis).

A Methodology for Identifying Perverse Incentives

The above examples illustrate how information security can be rife with problematic incentives. Their effect ultimately depends on how the future unfolds for the organization and the impact this has on the decision-makers of O. The approach we propose to deal with perverse incentives is described below and illustrated in Figure 1:

1. Make a list F of the possible futures, coarsely quantized – e.g., F = {"security breach", "no security breach"}.
2. For each relevant entity X in O, do the following:
    a. Make a list L(X) of the possible actions by X. L(X) too is coarsely quantized – e.g., "buy" or "sell", "invest" or "do not invest", "deploy" or "do not deploy", etc.
    b. For every pair of elements f,A from F and (resp.) L(X) (i.e., for each future-action pair), create a list C(f,A,X) of the consequences for X of that future-action pair, and a list C(f,A,O) of the

www.manaraa.com

consequences for O of that future-action pair. C(f,A,X) is created using the current reward system and policies of the organization O.

c. Compute the expected value, denoted E(A,X), of action A for X, as follows:

   i. Attach to each f,A a probability p(f,A,X) of occurrence of future f assuming action A, as that probability is perceived by X. For example, a probability p for a headline-making security breach, a probability q = 1-p of no such major breach. These are perceived probabilities based on either an interview with X or on surveys of people who hold jobs similar to that of X (e.g., system administrators, CISOs, etc), rather than computed probabilities based on factual historical data. We use subjective probabilities because they determine X's choices (humans form subjective opinions that can differ considerably from reality, and it is what X believes that matters when it comes to incentives, just like it was the fund manager's belief that mattered in example 1 – whether the belief is accurate or not was not an issue). Authors believe that subjective probabilities can be employed usefully in information security assessment, even when quantitative data is not available or a formal process description is not required. However, we wish to warn managers of some cognitive biases that stem from the reliance on judgmental heuristics, which may occur in subjective analysis. The origins of these pitfalls can be classified into three types: 1- Representativeness, 2-Availability, and 3-Adjustment and anchoring--for a detailed discussion see Tversky and Kahneman (1974).

   ii. Attach to each f,A a value v(f,A,X) that estimates the impact of C(f,A,X) on X (again, as perceived by X); that value is positive if X benefits and negative if X loses.

   iii. E(A,X) = the sum over all f in F of p(f,A,X)* v(f,A,X)

d. Compute the expected value, denoted E(A,O), of action A for O. This is done similarly to the previous sub-step (c) except that now the numbers used are objective and based on factual data. The rationale for this is that, whereas the actions of X may be (mis)guided by X's subjective judgments, their impact on O is more objective and based on historical data and precedent for O or for the industrial sector to which O belongs (e.g., banking).

e. If the action A' that maximizes E(A,X) differs from the action A" that maximizes E(A,O) then flag the reward policies that result in C(f,A,X) as potentially "perverse" and to be reviewed by the organization; the next sub-section discusses how they are handled.

www.manaraa.com

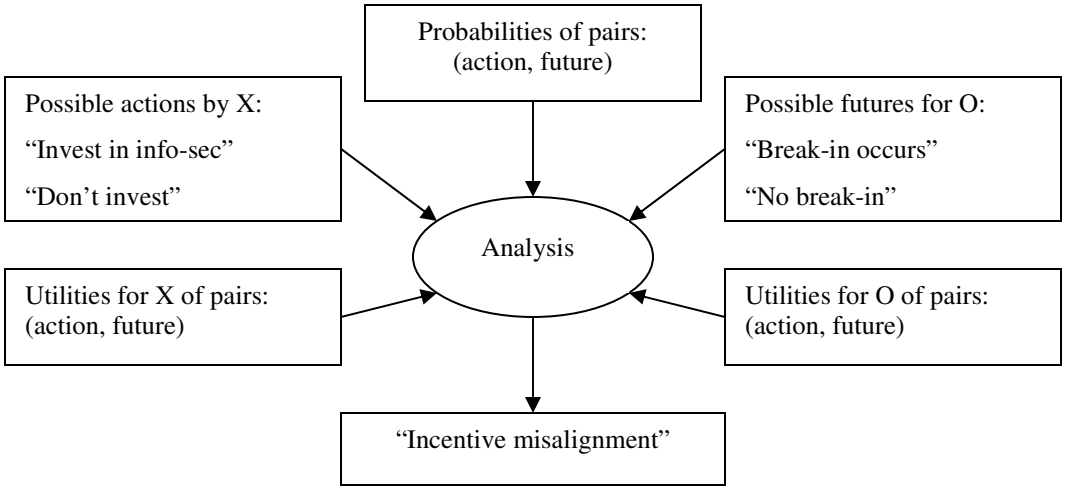

Figure 1. Illustrating the Detection of Perverse Incentives for a Manager X of an Organization O

Handling the Flagged Incentives

The review by the organization of the incentives flagged as potentially perverse in the above Step 2(e) may reveal that there is in fact nothing wrong with the policies (which is why we had tagged them as "potentially" rather than actually perverse). In the case of such a false positive, the mis-alignment of X's incentives with the interests of O is due to the mis-perception by X of the p(f,A,X)'s, of the v(f,A,X)'s, or of both. That is, these subjectively perceived quantities may differ substantially from the objective ones. In that case what is needed is not a change of the reward policies, but rather an education initiative to convey to X the objective probabilities and consequences.

A Caveat, and its Cure

Just like the mis-perceptions by X can cause the appearance of false positives, they can also cause false negatives – the mis-perceived (by X) probabilities and values cause X to make choices consistent with the interests of O. In such false negatives, there is a danger that X may suddenly re-assess the situation more accurately, and as a result may start acting against the interests of O. But these false negatives are easy to detect and correct by simply running the above algorithm using objective values for both X and O. But it is not clear that organizations may wish to correct such mis-perceptions if they work in their favor: Their very business model may depend on these mis-perceptions by both their employees and their customers. For example, an employee who over-estimates the odds that O will detect attempted fraud certainly need not be enlightened by O about the reality of the lower odds of being caught. The perception by every X in a unit of O that a break-in will cause X to be fired may not conform to reality (e.g., it is impossible to simultaneously fire everyone in the IT department), but it may be beneficial for the organization to foster such beliefs. This is why we recommend using subjective rather than objective values in the above-outlined methodology (we later below discuss the quantification of perceived risk, that is needed in the above methodology).

An Illustrative Example

The "computing facilities" manager X of an organization O gets a fixed yearly budget for expenditures that X can allocate to

a. Providing the additional software and hardware facilities requested by the other units of the organization, or
b. Hiring more staff to support the existing services, or
c. Deploying better security technologies and procedures.

www.manaraa.com

The unit managed by X gets a "satisfaction rating" by the other units of O on the quality and breadth of services that it provides, and that rating determines the salary raise of both the manager X and of every employee Y of the "computing facilities" unit. The allocation of resources between the above choices a,b,c is done democratically by a vote of the staff rather than by an edict from X, because the staff are most attuned to the needs and complaints of the customers of their unit (which are the other units of O). Should a serious security breach occur, X is likely to be fired because O cannot afford the compromise of sensitive data that would result from such a breach.

The perverse incentive in the above situation is readily identified when considering a staff member Y who works under X: The vote of such an individual Y is most likely to be skewed towards allocating resources to (a) or (b) but not to (c): To (a) because it results in higher customer satisfaction and a better raise for Y, to (b) because it lowers Y's work load, but not to (c) because it inflicts costs on Y who would have to support and maintain additional security software and procedures, the absence of which would endanger mostly X and O rather than Y (in the low-probability case that a security breach occurs it is X that gets fired, Y would suffer only a lower raise from the negative customer ratings). Note that the low-probability breach is intolerable to O, who has a vested interest in appropriate expenditures in category (c). The situation can be fixed by a number of changes (or a combination of them), the most plausible of which is that the allocation of resources would no longer be done by vote, but rather by an executive decision from X after consulting with the staff on the customer needs and complaints. The alternative of modifying the policy (or perception) that only X is fired in case of a breach is less plausible, because it is not practical to fire the whole computing facilities staff if a breach were to occur.

Stakeholder Perception of Information Security Risks

Previous studies show that perceived risk is quantifiable and predictable (Johnson and Tversky 1984; Slovic 1987). Psychometric techniques seem well suited for identifying similarities and differences among groups with regard to risk perceptions and attitudes. These studies have also shown that the concept of risk means different things to different people. When experts judge risk, their responses correlate highly with technical estimates of annual fatalities. Lay people can assess annual fatalities if they are asked to (and produce estimates somewhat similar to the technical estimates). However, their judgments of risk are related to more characteristics (e.g. catastrophic potential, threat to future generation). Our literature review indicates that unknown risk and dread risk can account for about 80 percent of the results generated by using all nine variables that were originally introduced by Fischoff and his colleagues (Fischhoff et al. 1978; Johnson and Tversky 1984; Slovic 1987).

Our first approximation model is based on the psychometric model of risk perception developed by Fischoff, Slovic and others, in which characteristics of a risk are correlated with its acceptance. For example, risks that are undertaken voluntarily are generally considered more acceptable than risks imposed without consent. Similarly, risks that cause dreaded forms of harm are also considered to be less acceptable. In our model, we condense Fischoff's nine variables of risk--voluntariness, immediacy of effect, knowledge about the risk (known by the person), knowledge about the risk (known to science), control over the risk, novelty, chronic or catastrophic, degree of dread, severity of consequences--by considering understanding (familiarity and experience) and consequences (scope, duration, and impact) as the two principal characteristics of information security and privacy risks. The authors argue that to measure these characteristics we need metrics that contain units of measure and some numerical scale. These scales should be *good enough* for managers to do a tradeoff analysis between perceived benefit and risk and capable of describing (Geer et al. 2003):

- How secure the organization is,
- Whether the organization is doing better or worse compared to the past,
- Whether the organization is spending the right amount of resources,
- How the organization compares to its peers, and
- What risk transfer options the organization has.

The most commonly used and preferred scale is *ratio scale*, where ordered data has a constant scale and a natural zero and ratios matter--10 is five times larger than 5. However, in information security there is not enough statistical data upon which to base the decision to assess the damages and to use ratio scale. Ordinal scales could be alternative, where the categories and the labels are still just categories and labels, but there is an unambiguous sense that there is a natural sequence to them as otherwise arbitrary as they are. In this research, we use an ordinal scale to

www.manaraa.com

measure the characteristics of perceptions of information security risks. We benefit from categories and labels introduced in Bloom Taxonomy (Bloom and Krathwho1956) and National Institution of Standards and Technology (NIST) Stonebumer (2002) in measuring these characteristics.

Alavi and Leidner (2001) have studied how to understand and manage knowledge in information systems by surveying the work of various authors (e.g. Carlsson et al. 1996; Schubert et al. 1998; Zack 1998). Such an understanding is needed for formulating an organization's knowledge management strategy and in characterizing information security and privacy risks. Figure 2 summarizes their findings. Here, the vertical axis represents understanding the differences among data, information, and knowledge and drawing implications from the differences.

Some tangible consequences can be measured quantitatively as lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other consequences (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of their effects. In Figure 2, the horizontal axis represents different levels of consequences. Thus, a point P in the figure represents a given risk perception in terms of its understanding and consequences.

The authors argue that a major problem with current approaches taken by senior management is that they do not address how to cope with changes in technologies, align their policies with these changes, and acknowledge the dynamic processes by which stakeholders learn about risk and choose among real life prospects with associated uncertainties, risks and benefits. We acknowledge the dynamics of perception by including a time element t in our model as follows:

$$P_{(t_1,t_2)} = f(U_{(t_1)}, C_{(t_1,t_2)})$$

$$Where: t_2 \succ t_1, \& t_1, t_2 \in [a,b]$$

$$U_{(t_1)} = \int_a^{t_1} U_{(t)}$$

$$C_{(t_1,t_2)} = \int_{t_1}^{t_2} C_{(t)}$$

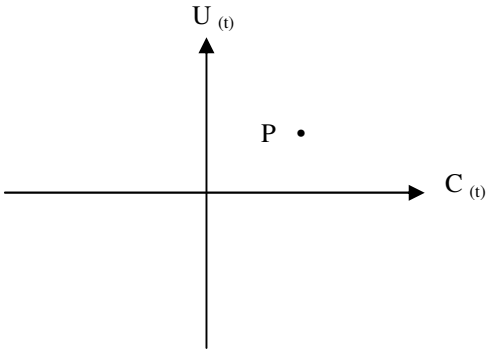

Figure2. Characteristics of Perceptions of Information Security Risks

In the model [a, b] represents a time interval that begins at some point a during the user's lifetime and ends at some point b in the future, representing how far forward the person observes the impact of the event. We define $P_{(t1, t2)}$ as the perception of the privacy loss over the time interval (t_1, t_2). $U_{(t)}$ and $C_{(t)}$ accordingly represent understanding and the consequences caused by the privacy incident (breach) at time t. In particular, we measure over an interval where the exposure may occur at time t_1 and consequences accrue until time t_2. For the first dimension of the model, addressing consequences of the breach, we can posit scenarios to explore the fear stakeholders have of the potential effects of the risk of information security losses. These issues fall into three main categories, as shown in Table 1.

www.manaraa.com

Table 1. Issues about Consequences

Category	Issue
How serious are the effects?	• How serious is the potential harm thought to be, in dollar value, loss of time, and stress? • Are the effects potentially catastrophic? Can one error lead to financial ruin? • Are the effects overt or hidden? (Hidden effects are usually more feared)
How long term are the effects?	• How immediate are potential effects? (Delayed effects are usually more feared) • Are the effects reversible?
How feared are the effects?	• Are the effects unusual or outside of normal experience? • Do views differ among population subgroups for demographic or other reasons? • Do the view of the exposed group, differ from those who don't ?

Analyzing these responses to the survey enables us to assign one of the following five levels to the consequence dimension:

- Level 1: Effects are trivial, temporary and commonplace
- Level 2: Effects are potentiality serious but treatable
- Level 3: Effects are serious, long term but considered natural
- Level 4: Effects are serious, ongoing and raise ethical concerns
- Level 5: Effects are catastrophic, ongoing and highly feared

Definitions of "trivial," "serious," and so on are based on those in Stonebumer (2002). Level 5 and level 1 represent the highest and lowest level of consequences, respectively. These five levels of consequences have been defined based on scope (local or global), duration, and impact of the security incident. For the second dimension, reflecting understanding, we can ask questions to explore cognitive understanding of the risk's cause-effect, and others that attempt to uncover the factors motivating users to attend to certain risks while dismissing others. These questions are intended to identify affective factors that influence users' cognitive understanding of the cause and effect. The issues fall into two main categories as shown in Table 2.

Table 2. Issues about Understanding

Category	Issue
Who (among the user group) understands the hazard?	• Is understanding confined to certain (e.g. special interest) members? • Is there agreement on risk mechanisms or are there conflicting views?
What do they know?	• How well is the cause-effect mechanism understood and why? • Is understanding complete or partial? • Where understanding is partial: 1. Are there similarities to existing, understood risks? 2. Does substantial disagreement exist about fundamental aspects of the cause-effect mechanism? 3. Can the cause-effect mechanism be quantified confidently and used to predict risks accurately?

Our theoretical framework for categorizing understanding is based on the work of Bloom and Krathwhol (1956). Here, we are interested in understanding of risk causes and effects using the cognitive domain and what contributes

www.manaraa.com

to their motivation to acquire understanding using the affective domain. Answering these questions will help us in assigning one of the following six levels to the understanding dimension (Farahmand et. al. 2007):

- Level 1: Evaluation: Make judgments about the value of ideas or materials.
- Level 2: Synthesis: Build a structure or pattern from diverse elements. Put parts together to form a whole, with emphasis on creating a new meaning or structure.
- Level 3: Analysis: Separate material or concepts into component parts so that its organizational structure may be understood. Distinguish between facts and inferences.
- Level 4: Application: Use a concept in a new situation or unprompted use of an abstraction. Apply what was learned in the classroom to novel situations in the workplace.
- Level 5: Comprehension: Understand the meaning, translation, interpolation, and interpretation of instructions and problems. State a problem in one's own words.
- Level 6: Knowledge: Recall data or information.

Level 6 and level 1 represent the lowest and the highest level of understanding, respectively. In the presented model, the perceived risk increases whenever the score increases; when consequence increases and understanding drops. This model was discussed and verified with thirty five senior information security executives from industry and governmental organizations across the country in one-on-one meetings in the past twelve months. These executives had at least 10 years of experience and in the course of their experience had dealt with a large range of information security--human and computer related--issues. Following a ten-minute --in average--description of our model, they were able to map their experiences into the model, to describe those experiences in different levels of consequents and understanding, and to evaluate the change of the perceptions of risk--by different stakeholders--in the course of the time.

The following are generic examples where stakeholders are victimized. Parallel examples would involve people who were not victimized but who might be concerned.

> *Example 1- Stealing identity for credit card fraud.* As the first incidents occur, stakeholder's understanding is low at first --levels 5 and 4 of "U" dimension. Understanding increases with time, and reaches a maximum--Levels 2 and1. Thereafter, there is little increase for subsequent incidents. Typically, there may be a sudden increase in consequences--from level 2 to level 4 of "C" Dimension-- which may either grow or decrease with time, depending on the kind of fraud perpetrated. Privacy loss may increase with time as the victim is required to expose more details to recover, but eventually the loss subsides to a steady-state of lasting privacy loss.
>
> *Example 2- Medical records disclosed to improper third party.* Understanding by the victim is likely to be low --levels 6 and 5 of "U" Dimension--and may not increase. Consequences could range from very low--level 1 of "C" Dimension-- to eventual extortion--level 6 of "C" Dimension-- if the data contain information whose revelation is embarrassing. The victim may file legal claims and recover some recompense, so the damage could peak and then decline.

When there is more than one type of risk event associated with a relationship between the stakeholder and the organization, aggregation becomes an issue. For example, in web-based credit card transactions, the stakeholder may perceive several types of risk, such as identify theft by someone snooping on the stakeholder's home wireless network, mass identify theft at the merchant by a disgruntled employee, double billing by the merchant, inability to get prompt refunds for wrong merchandise, etc. Aggregation of the responses over several events can be achieved by one of various methods, including weighted linear combination, geometric combination, or maximum value. The issue of aggregation is one that will be further investigated parting future installments of this research.

www.manaraa.com

Conclusions and Further Research

Information systems deal with a large set of potential risks, with an equally large (or larger) set of possible losses. Losses can include damage to or loss of physical systems, employee time, subtle corruption of data, loss of privacy, and loss of an organization's reputation for care and accuracy, etc. Senior management seeking to mitigate the full set of risks must assess the system for all of these potential losses. Furthermore, senior management must also address the perceptions of risk that may be held by all stakeholders that could be different. Although all risks may be addressed, if stakeholders fear that the system exposes their personal data they may be afraid to use it. As experience shapes user perceptions they become proxies of actual risk. They may actually be good predictors of risk in the absence of better methods. Even if this is not a precise process, sound management practice dictates that it address user perceptions. Senior management in choosing policies should realize that stakeholder perceptions of uncertainties, risks, and benefits have major impact on the acceptability of the proposals. Therefore, perceptions should enter into the evaluation of incentives, and probabilities of final outcomes.

It is incumbent on the senior management team and the board to consider possible security risk threats, means and controls for prevention of breaches, isolation and minimization of damage and recovery and renewal of operational stability. The confusion of mis-directed perceptions, ill-advised allocation of decision rights and failure to assess the mix of controls may result in significant exposure for the enterprise.

It is the understanding of the incentives and desired outcomes that permit the allocation of decision rights and authorities to deal with the day-to-day decisions that face the management team. The framework presented permits the illumination of appropriate factors for alignment of the interests of all parties.

We are currently exploring ideas that there are two changes in the manner in which we make decisions about technological enterprises that would simplify: change in attitude, and change process. Managers must first recognize that the gap between experts and lay stakeholders will not be narrowed by forcing change only on the part of the lay stakeholders alone. The respect that lay stakeholders once held for experts will be restored only if experts work at reversing an image that makes them appear to be self-serving, dangerous opponents. One approach for managers to this reversal would be for the experts to develop an appreciation and an understanding of lay stakeholder perceptions of the risks of technology and to accept the fact that these perceptions play an important role in decision making.

The need to increase information security literacy is a high priority in the information age. A dominant method for increasing literacy in any field is through awareness, training, and education programs intended to develop the knowledge and skills required of information-literate citizens. Examples of such programs for the masses include Stay Safe Online, NetSmartz, and Cyber Safety. Despite the need for an information-literate public and the development of such programs, we contend that a great deal more is needed to change attitudes and inform the public about risks associated with information technology.

With the ever changing nature of the network environments, questions arise that transcend any current network technologies. It is incumbent on our studies of organization, networks and inter-organizational practice to facilitate secure environments for commerce. Our program of research in these areas balance the interests that are technical, social and organizational state some of the key questions:

- How do we quantify risk of information security incidents?
- How do we best investigate information systems security incidents and subsequent damages?
- How do we select appropriate control measures to ensure effectively support risk management?

These questions matter to all stakeholders, their comfort and trust in the employment and engagement of the network environment, the procedures, and practice in their daily commerce.

www.manaraa.com

Acknowledgments

This material is based in part upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College. Portions of this work were supported by Grant CNS-0627488 from the National Science Foundation, and by sponsors of the Center for Education and Research in Information Assurance and Security. The authors would also like to acknowledge the contribution of Professor Eugene H. Spafford, Professor Melissa Jane Dark, and Dr. Shari Lawrence Pfleeger for their contribution in model of risk perception presented in this paper

References

Alavi, M., and Leidner, D. E. "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research issues," *Management Information Systems Quarterly*, Vol. 25, No 1, March 2001, pp. 107-136.

Alhakami, A., S. and Slovic p. "A Psychological Study of Inverse Relationship between Perceived Risk and Perceived Benefit," *Risk Analysis*, Vol. 14, No. 6, 1994, pp. 1085-1096.

Anderson, R. *Security Engineering*, Second edition, Wiley, 2008.

Anderson, R., and Moore, T. "The Economics of Information Security," *Science*, 314 (5799), October 27, 2006, pp. 610–613.

Anderson, R., "Why Information Security is Hard: An Economic Perspective", Proceedings of the *Seventeenth Computer Security Applications Conference*, IEEE Computer Society Press (2001), I pp. 358-365.

Bloom, B. S., and Krathwohl, D. R. *Taxonomy of educational objectives: The Classification of Educational Goals,by a Committee of College and University Examiners. Handbook 1: Cognitive domain*, New York, Longmans, 1956.

Carlsson, S. A., El Sawy, O. A., Eriksson, I., and Raven, A. "Gaining Competitive Advantage Through Shared Knowledge Creation: In Search of a New Design Theory for Strategic Information Systems," in *Proceedings of the Fourth European Conference on Information Systems,* J. Dias Coelho, T. Jelassi, W. Konig, H. Krcmar, R. O'Callaghan, and M. Saaksjarvi (eds.), Lisbon, 1996.

Diamond, L. "The Impact of Information Form on the Perception of Risk," *International Conference on Information Systems*, 1988, pp. 91-97.

Dynes, S., Goetz, E., and Freeman, M. "Cyber Security: Are Economics Incentives Enough?," *IFIP International Federation for Information Processing,* Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; 2008, (Boston: Springer), pp. 15–27.

Ernest & Young. *Managing Risks Stakeholders Perspective*, Ernest & Young, 2005.

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

Farahmand, F., Spafford, E. H., and Dark, M. J. *Understanding Stakeholder Perspective of Risk in Designing Information Security Policies*, 2007, CERIAS Report Number: 2007-93.

Finucane, M. L., Alhakami, A., Slovic, P., and Johnson, S. M. "The Affect Heuristic in Judgments of Risks and Benefits," *Journal of Behavioral Decision Making*, 2000, Vol. 13, pp. 1-17.

Fischoff, B., Slovic, P., Lichtenstein, S., Read, S., and Combs, B. "How Safe Is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits?" *Policy Sciences,* 9(2), April 1978, pp. 127-152.

Geer, D. "A Quant Looks at the Future," *CERIAS Information Security Symposium Keynote Address*, Purdue University, March 2007.

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

www.manaraa.com

Gefen, D., P., and Pavlou, P. A. "The Modeling Role of Perceived regulatory Effectiveness of the Online Marketplaces on the Role of Trust and Risk Transaction Intensions," *International Conference on Information Systems,* WI, 2006.

Gibbons, R. "Incentives in Organizations," *The Journal of Economic Perspectives*, Vol. 12, No. 4, (Autumn, 1998), pp. 115-132.

Gordon, L., A. *Incentives for Improving Cybersecurity in the Private Sector: A Cost-Benefit Perspective,* Testimony for the House Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Oct 2007.

Gordon L. A., and Loeb, M. P. "Return on Information Security Investments," *Strategic Finance*, Nov. 2002, pp. 26-31.

Goodhue, D. L., and Straub, D. W. "Security Concerns of Systems users; A Study of Perceptions of the Adequacy of Security," *Information & Management*, Vol. 20, 1991, pp. 13-27.

Hu, X., Lin, Z., Whinston, A., and Zang, H. "Perceived Risk and Escrow Adoption," *International Conference on Information Systems,* 2001, pp. 271-274.

Johnson, E. J., and Tversky, A. "Representations of Perceptions of Risk," *Journal of Experimental Psychology*; General. 113, 1984, pp. 55-70.

Kahneman, D., Ritov, I.,and Schkade, D. "Economic Preferences or Attitude Expressions?:" An Analysis of Dollar Responses to Public Issues," *Journal of Risk and Uncertainty*, 1999, 19:1-3; pp.203-235.

Kerr, S. "On the Folly of Rewarding A, While Hoping for B," *The Academy of Management Journal,* Vol. 18, No. 4, (Dec., 1975), pp. 769-783.

Kim, K., and Prabhakar, P. "Initial Trust, Perceived Risk, and the Adoption of the Internet Banking," *International Conference on Information Systems*, 2000, pp. 537-543.

Lazear, E. P. "The Power of Incentives," *The American Economic Review,* Vol. 90, No. 2, Papers and *Proceedings of the One Hundred Twelfth Annual Meeting of the American Economic Association*, May 2000, pp. 410 - 414.

Loch, K., Carr, H., and Warkentin, M. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, 17 (2), 1992, pp 173-186.

March, J. G., and Shapira, Z. "Managerial Perspectives on Risk and Risk Taking," *Management Science,* Vol. 33, No. 11, 1987, pp. 1404-1418.

Moores, T. T., and Dhillon, G. "Do Privacy Seals in E-Commerce Really Work?," *Communication of ACM*, Dec. 2003/Vol. 46, No. 12, pp. 265-271.

Odlyzko, A., "Privacy, Economics, and Price Discrimination on the Internet," *Workshop on the Economics of Information Security*, 2003.

Payne, J., Bettman, J. R., and Johnson, E. "Behavioral Decision Research: A Constructive Processing Perspective," *Annual Review of Psychology*, 1992, 43, pp. 87-131.

Prendergast, C. "Incentives in Organizations," *The Journal of Economic Perspectives*, Vol. 12, No. 4, (Autumn, 1998), pp. 115-132.

Raiffa, H. "Concluding Remarks," in Societal Risk Assessment; How safe is safe Enough, Edited by Schwing, R. C., Albers, W. A., *Proceedings of the General Motors Symposium on Societal Risk Assessment,* Oct. 1979, pp. 339-341.

Schkade, D. A. and Johnson, E. J. "Cognitive Processes in Preference Reversals," *Organizational Behavior and Human Decision Processes*, 1989, Vol. 44, pp. 203-231.

Schubert, P. Lincke, D., and Schmid, B. "A Global Knowledge medium as a Virtual Community: The NetAcademy Concept," *Proceeding of the Fourth Americans Conference on Information Systems,* Aug 1998, pp. 618-620.

Slovic P., Finucane, M. L., Peters, E., and MacGregor, D.G. "The Affect Heuristic," *European Journal of Operational Research*, 2007, 177, pp. 1333-1352.

Slovic, P. 1987. "Perceptions of Risk," *Science*, 236, 1987, pp. 280-285.

Slovic, P., and Lichtenstein, S. "Relative Importance of probabilities and Payoffs in Risk Taking," *Psychology Monograph*, Vol 78, No 3, part 2, 1968, pp. 1-18.

Stewart, A. "On Risk, Perception and Direction," *Computers & Security*, Vol 23, 2004, pp. 362-370.

Stone, W. S. and George, G. "On the Folly of Rewarding A, while Hoping for B: Measuring and Rewarding Agency Performance in Public-Sector Strategy," Public Productivity & Management Review, Vol. 20, No. 3, (Mar., 1997), pp. 308-322.

Stonebruner, G., Gougen, A., and Feringa, A. *Risk Management Guide for Information Technology Systems,* NIST SP800-30, 2002.

www.manaraa.com

Straub, D. W., and Welke, R., J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly,* 22:4, 1998, pp. 441-469.

Straub, D. W., Goodman, S., and Baskerville, R. "Promising Future Research in Infosec," *in Information Security; Policy, process, and Practices,* edited by, Straub, D. W., Goodman, S., & Baskerville, R., M. E.Sharpe, 2008, pp. 263-274.

Taylor, R. G. "Management Perception of Unintentional Information Security Risks," *International Conference on Information Systems,* 2006, pp. 1581-1597.

Tversky, A., Sattath, S., and Slovic, P. "Contingent Weighting in Judgment and Choice," *Psychological Review*, Volume 95(3), July 1988, p 371–384.

Tversky, A. and Kahneman, D. "Judgment and Uncertainty: Heuristics and Biases," *Science*, New Series, Vol 185, No. 4157, Sep. 1974, pp. 1124-1131.

Varian, H., "Managing Online Security Risks Economic Science", Column, The New York Times, June 1, 2000.

Wash, R., and MacKie-Mason, J. K. "Incentive-Centered Design for Information Security," *1st USENIX Workshop on Hot Topics in Security*, 2007, pp. 1-6.

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

Zack, M. "An Architecture for Managing Explicated Knowledge," *Sloan Management Review*, September 1998.

Zajonc, R. B., "Feeling and Thinking: Preferences Need no Inferences," *American Psychologist*, Vol. 35, 1980, pp.151-175.

www.manaraa.com