Intelligent Information Management, **2011, 3, 112-118**
doi: 10.4236/iim.2011.34013 Published Online July 2011 (http://www.SciRP.org/journal/iim)

Risk Management in On-Line Banking

Ioannis Koskosas
University of Western Macedonia, Kozani, Greece
E-mail: ioanniskoskosas@yahoo.com

Received February 7 2011; *received May* 6, 2011; *accepted May* 15, 2011

Abstract

In the context of goal setting, the more difficult the goal, given feedback on performance, the more focused is individuals' attention and persistence to accomplish the goal and in turn, their performance is also improved. Similarly, when the goal is multi-complex and performance time constraint, the deployment of specific strategies maybe the best approach developed. In effect of the above, this investigation takes a socio-psychological and organizational perspective in setting information systems (IS) security goals. In doing so, three important issues of goal setting are identified, these are: trust, culture and risk communication. Since system security breaches are still on the rise, the performance of managing such online risks is not the one expected. The framework suggested in this paper aims to contribute to socio-psychological and organizational values by enhancing the performance of the IS risk management process with a focus on security risks.

Keywords: Online Banking, Trust, Culture, Risk Communication, Goal Setting

1. Introduction

The research described in this paper is concerned with Information Systems (IS) security. IS security has become an important issue for companies and individuals as access to information has become easier through closed network (dial-up) communication lines and later to the general public with the introduction of the Internet [1]. In the U.S.A., in 2000, 85% of 538 survey respondents reported security breaches; in 2001, 36% reported incidents of cyber-crime, up from 25% in 2000 and 16% in 1999 [2]. In Europe, a report by the London-based research firm Datamonitor says that European firms have been particularly lax in protecting themselves from security threats; and while Datamonitor projects that international security spending will reach $30.3 billion by 2005, more than 50% of 300 CIOs and IT directors from across Europe reported that security spending accounted for 5% or less of their IT budgets in 2000 [3].

The above results indicate that security issues, particularly in Europe are more discussed than practiced. Risk management appears to be partially neglected with a negative effect on performance. Many research studies have developed new security approaches and techniques for managing risks but it appears that ignore the social aspects of risks and the informal structure of organizations [4,5,6]. This paper investigates security risks from the non-technical point of view. In the next section the theory of goal setting is introduced and the concepts of trust, culture, and risk communication are discussed as their role in the process of goal setting is valuable.

2. The Growth in On-Line Banking

On-line banking aims to provide easy access to banking services for customers. Both banks and customers stand from the introduction of on-line banking to benefit schemes, since the bank can offer its services at much lower cost, while the customer can access the services from any location at any time.

However, the developments of on-line banking activities have altered the nature and scope of security risks faced by the banking industry as well as the speed with which risk exposures can change. In addition, on-line banking is an area of highly leveraged information, and risk manipulation and dissemination is one of the main concerns of managers [7].

In the same vein, the on-line industry and particularly Web banking, is becoming an increasingly large and significant market.

However, on-line banking is not restricted to Web banking but also includes ATMs, Tele-phone banking, Mobile banking, and TV banking. The continued popularity of cash transactions is reflected in the growth of

European automatic teller machines (ATMs) market to more than 250,000 machines during the year 2000 [8]. UK, Germany, Spain and France each have 30,000 installations and account for three quarters of the region's total while Greece and Portugal showed the fastest percentage growth [8].

According to RBR survey, on average, there are 554 ATMs per million population in Western Europe although this number is much lower than in the U.S.A. and Japan, where there are more than 1000 machines per million people.

Telephone banking has a tremendous amount of potential, given the fact that 97% of American's 94 million households have a touch-tone phone [8]. Telephone banking allows customers to check their status of accounts whenever they want, any time of the day or night. Every activity that can be handled in a branch (with the exception of cash) should be available via the telephone.

Mobile banking services through the wireless device combine short message service (SMS) and WAP, which is also being used to deliver secure interactive banking services to pay bills, check account balances and stock information through a preconfigured mobile phone usually lining them to bank's services [9]. WAP (wireless application protocol) is already facilitating secure, convenient, on-line shopping of the development and imminent launch of GPRS (general packet radio service) and UMTS (universal mobile communications system) services [9].

TV banking is another on-line delivery channel which is attracting the interest of the financial market. This is mainly because the costs involved in deploying this service (if not product) is lessen to other delivery channels as the costs are shared with TV network companies and of course, the consumer [10]. The on-line banking service available through Sky TV is an example of a major financial services company delivering services over interactive digital TV.

Although on-line banking is capturing a significant market share, the risk exposures, usually of security nature, that come along with the development of on-line banking activities need careful strategic planning. Thus, the aim of this investigation is to suggest a theoretical framework that might provide an alternative approach in thinking the organizational values, in terms of strategic planning, and to enhance the performance of risk management on security risks. In the following, the authors introduce the theory of goal setting. In doing so, they discuss the importance of goals and the critical role of commitment to goals in the process of goal achievement.

3. Conceptual Background

The concept of goal setting falls within the broad domain of cognitive psychology and its literature is extensive. The theory, as the name implies, is based on the concept of goals and is an essential element of social learning theory [11] which has become increasingly influential through time [12]. Locke (1977) agues that even the literature on organizational behaviour modification can be interpreted largely within a goal-setting framework [13,14].

In a similar vein, in order to understand and explain the effect of goals on action needs to understand the mechanisms by which goals produce their outcome [15]. According to Locke and Latham (1990), the three most direct goal mechanisms are primarily motivational [15]. They correspond to the three attributes of motivated action and these are:

- arousal or intensity
- choice or direction
- and duration.

Goals affect arousal by regulating the intensity of effort the individuals spend on the task and duration by leading people to persist in their actions until the goal is reached [15]. Goals affect also choice by leading people to direct their attention and take action with respect to goal-relevant activities [15].

However the main assumption of goal-setting research is that goals are immediate regulators of human action although the degree of association between goals and action remains an empirical question because people may, for example, make errors, lack the ability to attain their objectives or have subconscious conflicts that subvert their conscious goals [12]. This might be the case in dynamically complex task environments such as software development [16].

3.1. The Importance of Goals

The importance of goals with respect to work behaviour is well documented by two main propositions. These are:

- Increases in the difficulty of assigned goals leads to increases in performance (assuming goal acceptance)
- Specific, difficult, assigned goals result in higher performance than do best or no assigned goals

In the first proposition, a linear relationship between goal difficulty level and job performance is predicted, given that goals are accepted by the individual [14]. Over 90 percent of almost 200 studies support this proposition with effect size on performance being about a 10-15 percent increase as a result of goal level [15]. Based on the same number of studies plus one by Hunter and Schmidt (1983), 90 percent of these studies support the second proposition as well; in this case, the effect sizes ranged from 8-16 percent on performance [17,14].

In the same vein, Locke and Latham (1990) through an extensive review of the micro-literature on goals and task strategies, concluded that setting or accepting specific, challenging goals as compared to specific, easy goals or a goal of doing your best leads to [18]:

- More spontaneous development or use of task strategies [19,20]
- More spontaneous planning [21,22]
- Greater use of strategies that are provided to the subjects indirectly, through priming [22,23], or directly through formal training
- The development of better analytic strategies [24] that in turn enhance the quality of decisions.

Past research also shows that assigned goals influence performance through two types of mechanisms: those having a direct effect (*i.e*. effort, persistence, and directional attention) on an individual and those having an indirect effect (*i.e.* strategy development) [25]. As tasks become more complex, these mechanisms become progressively less adequate by themselves to ensure goal achievement, while the development of specific task strategies becomes progressively more important.

An important distinction between these two types of effects is that the direct effect is primarily motivational by allocating the individual's energy-related resources to task performance, whereas the indirect effect is primarily cognitive by developing a plan or strategy in order to use the mobilised, energy-related resources [25].

3.2. Goal Commitment

Locke and Latham (1990) refer to intensity as goal commitment, the degree to which the person sees the goal as important, is attached to it and determined to reach it, even in the face of setbacks, distractions or obstacles [14,15]. When the effects of commitment need to be measured, it is necessary first to establish goal level measures since variations in commitment may entail variations in goal level [15]. By saying that, it is also necessary to consider that when multiple goal levels are employed the overall correlation of commitment and performance across goal levels might be negative [26]. The reason for that is because very difficult goals which tend to increase performance, are generally less accepted than easy goals, which tend to reduce performance [15].

However commitment is related to performance in two aspects. Either if the goal level is held constant or in a sample if all participants were given the same challenging goal, commitment could have a direct positive effect on performance [15].

In the same vein, when the goal level varies among individuals commitment might moderate the effect of goals on performance [15]. That means the goal level among individuals with high commitment should be higher and positively related to performance than among those with low commitment to the goals.

4. Critical Factors in the Process of Goal Setting (CFGS)

Having introduced the theory of goal setting this section deals with the factors that are critical in the process of goal setting within the risk management process. Generally speaking, risk management in the social context is defined as a systematic process for the identification and evaluation of pure loss exposures faced by an organization or individual and for the selection and implementation of the most appropriate techniques for treating such exposures [27]. Risk management maybe the most vital process within any organization whereas the human capital allocated within that process plays an important role.

In order to effectively allocate, then, this human capital within the risk management process, it might be necessary first to know what is peoples' perception of risks (culture), establish trust, and ensure the communication of risks among the members of the risk management process is effective.

4.1. Culture

Understanding the culture of an organization helps to understand how people perceive risks and whether they belong to an individualist and/or collectivist group. Hence this is important since peoples' perception of risks will determine the security goals that need to be achieved. Individualist cultures are those where "individuals are loosely connected, and everyone looks after their own interests or those of their immediate family" [28, p.38]. Individuals have personal goals that might or might not overlap with those of their in-groups; in effect, they might put their personal goals first [29,29]. People in individualistic societies feel autonomous, and members of these societies emphasise the 'I', the 'this interests me' [30]. In such cultures the emotional dependency is more emphasised and stress is on an individual's goals.

Collectivism refers to the opposite pattern, representing cultures "in which people from birth onwards are integrated into strong, cohesive in-groups, which throughout people's lifetime continue to protect them in exchange for unquestioning loyalty" [28, p.38]. In collectivist societies, the group is important and there is a need for shared activity and group solidarity [31,28]. Obligations and duties override personal preferences, as the 'we' now dominates [30]. While collectivist societies are keen to protect and help their in-group members they are not necessarily so helpful to those outside this group. Group boundaries are explicit and firm, with collectivism representing an ‘in-group egoism’ [28].

4.2. Trust

The concept of trust has received attention in different social science literatures such as psychology, sociology, political science, economics, anthropology, and sociobiology [32]. In their research Porta *et al.* (1996) reviewed several studies on trust. These studies argue that trust determines the performance of a society’s institutions and according to them trust is a propensity of people in a society to co-operate in order to produce socially efficient outcomes [33].

Misztal (1998) suggests that the literature on sociological concepts of trust can be grouped into three [34]:

- Individual attributes such as feelings, emotions, and values
- Social attributes such as common goal to be achieved by an organization
- Public value such as institutional trust

Ratnasingham (1998) argues that trust is an important element in any trade transaction [35]. Since information is seen as one of the most valuable assets of an organization [36], trust plays a critical role in any transaction of information.

4.3. Risk Communication

Backhouse and Dhillon (1995, 1996) argue that security breaches occur when communication breaks down. In their analysis of communication break downs in organizations, they focus in finding out what happens rather than what should happen [38,36].

Bener (2000) supports that effective communication of risks is a difficult task when it is communicated to diverse audiences who hold different values and references with respect to risk events communicated [37]. Although there is a constant communication of risk between the participants of the risk management process, at times, it becomes critical to pass the ‘message’ across by one side as well as by the other side.

However the U.S.A. National Research Council defines risk communication as a component of risk management, which actually is selects the risk control options and provides the information upon which the government, industry or individual decision-makers base their choices [37].

In a similar vein, Krimsky and Plough (1988) argue that risk communication is not the only exchange of information between the involved parties, but also among the wider institutional and cultural contexts within which risk messages are formulated, transmitted, and embedded [39].

5. The Framework

The theoretical framework is based on the theory of goal setting and the theories of trust, culture and risk communication have an essential role in the process of setting security goals. In previous section, it was outlined that the relationship among goal level, commitment and performance are complex, including both direct and moderator effects [15,40]. It appears that when the goal level is held constant there are direct effects of commitment on performance. Thus, goal commitment is important in producing positive performance and the commitment needs to be high, especially where goals are moderately or extremely difficult [14].

The encouragement and support given by managers helps one think they can reach a goal, and one’s trust in these people is essential [14]. Supervisors and managers also have the legitimate authority and power to set goals and employees want to meet these expectations [15]. Group members and social influence are also essential as it is the public nature of the commitment and the instrumentability of the goal for reaching valued outcomes [14].

Figure 1 suggests a theoretical framework. At the bottom of the pyramid, trust denotes the importance of setting up security goals and denotes the foundation upon which the other levels can only be set up. At this level managers have to make sure that trust among the group exists to a certain degree. A level up is the culture which gives information on how people react to risks and generally speaking, what is their perception of risks. Risk perception from a social sciences point of view, assumes that risk is inherently subjective and human beings have invented the concept of risk to help them understand and cope with the dangers and uncertainties as well as to maximize expected values [41,42]. Establishing trust among the members of the risk management group allows the identification of the group’s culture. Communication of risks is also essential in setting up meaningful security goals and keeping constant the group’s commitment to the goals. Communication is at the third level of the pyramid and can only be in existence if the previous levels exist.

Risk communication, culture, and trust are essential concepts when the risk management process has to be synthesised and security goals to be set up. This is because at the level of goal setting it is essential an priority to establish trust among the participants of the risk man agement process, understand how people react to risks in order to find solutions to complex problems [43], and

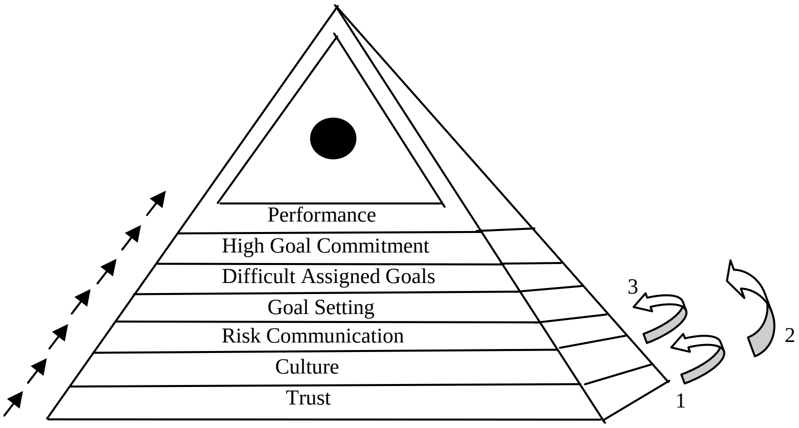

Figure 1. Performance Pyramid.

identify in advance any possible breaches in the communication process [39,36]. Further, this will assist in setting carefully the security goals to be achieved relative to the potential of the risk management group.

After these levels have been defined and established, the risk management group is in a position to identify and set on-line security goals that have to be achieved. According to the theory of goal setting in complex task environments, if people are assigned specific, and challenging goals (given goal acceptance) the task performance will increase compared to easy goals, "do your best" goals, or no goals [12]. Early *et al.* (1990) found also that "subjects" with specific, hard goals and feedback chose better strategies on a complex task than "subjects" without such goals and feedback [21]. Goals, therefore, affect performance by directing attention, mobilizing effort, increasing persistence, and motivating strategy development [12].

In the same vein, goal level, commitment, and performance have a complex relationship including direct and moderator effects [40]. When the goal level is held constant it appears that there are direct effects of commitment on performance. For difficult goals the relationship is positive while for easy goals it may be negative [12]. The moderating effects, across goal levels, shows that commitment is especially important when goals are difficult [14]. That means the relationship between goal level and performance is stronger with high commitment than with low commitment. In the same line of reasoning, in complex, and dynamic environments such as the risk management process, high commitment should increase performance with a focus to on-line security risks.

6. Conclusions

As the developments of on-line banking activities continue to grow, security risks inherent in the nature of on-line financial transactions should become even of more concern to financial institutions. Why? Because its not (financially) efficient, on the one hand, the annual spending on security measures to be expected to grow from $8.7 billion in 2000 to $30.3 billion in 2005 [44] and, on the other hand, the security breaches reported by firms to be still in existence and especially at a high rate of frequency. Maybe Dhillon and Backhouse (2001) are right when they suggest that most security approaches tend to offer narrow, technically oriented solutions, whereas managing security needs in the context of information systems needs a socio-organizational approach [6,5,45].

This investigation, thus, suggested a theoretical framework drawn from cognitive psychology in order to contribute to socio-organizational values and to enhance the performance of the IS risk management process with a focus on security risks. Within the risk management process, at the level of goal setting, it was recognized that managers before deploy their strategies to achieve their goals they should consider the concepts of trust, culture, and risk communication. After these levels have been defined, managers can be in a position to understand the security needs of their on-line banking systems and develop the necessary strategies to respond to such risks. It is out of the scope in this paper to refer to the best possible methods that might be used for the analysis of security requirements of on-line banking systems. The scope of this paper is to give useful insights into the risk management process by deploying a goal setting approach that focuses to on-line banking security risks.

7. References

[1] R. V. Solms, "Information Security Management: Why

Information Security is So Important." *Information Management and Computer Security*, Vol. 6, No. 4, 1998, pp. 174-177. doi:10.1145/162124.162127

[2] R. Power, "CSI/FBI Computer Crime and Security Survey," *Computer Security: Issues and Trends*, Vol. 11, No. 1, pp. 1-20.

[3] S. Jasanoff, "Learning from Disaster: Risk Management after Bhopal," University of Pennsylvania Press, Philadelphia, 1994.

[4] R. Baskerville, "Information Systems Security Design Methods: Implications for Information Systems Development," *Association for Computing Machinery Computing Surveys*, Vol. 25, Vol. 4, 1993, pp. 375-414. doi:10.1145/162124.162127

[5] G. Dhillon and J. Backhouse, "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal*, Vol. 11, No. 2, 2001, pp. 127-153. doi:10.1046/j.1365-2575.2001.00099.x

[6] W. E. Jacoby, "Strategic Information Systems Planning and Implementation in the U.S. Financial Services Industry," University of London, London, 1995.

[7] D. Hirsch, "The Future of Cash in Europe," *ESTA Conference Proceedings*, Tallin, 2007.

[8] P. Bansal, "Mobile Banking Steps up a Gear." *The Banker*, Vol. 151, 2001, pp. 121-126.

[9] N. Huber, "XML Cracks TV Banking Service: Company Business and Marketing," Computer Weekly, Reed Business Information, 2000, pp. 51-52.

[10] A. Bandura, "Self-efficacy: The Exercise of Control," Freeman Publishing, New York, 1977.

[11] E. A. Locke, L. M. Saari, K. N. Shaw and G. P. "Latham, Goal Setting and Task Performance: 1969-1980," *Psychological Bulletin*, Vol. 90, No. 1, 1981, pp. 125-152. doi:10.1037/0033-2909.90.1.125

[12] E. A. Locke, "The Myths of Behaviour Mod in Organizations." *Academy of Management Review*, Vol. 2, 1977, pp. 543-553.

[13] T. R. Mitchell, M. Thompson and J. George-Falvy, "Industrial and Organizational Psychology," Blackwell Publishers, Oxford, 2000.

[14] E. A. Locke and G. P. Latham, "A Theory of Goal Setting and Task Performance," Englewood Cliffs, New Jersey: Prentice-Hall, 1990. pp. 413.

[15] R. H. Rasch and H. L. Tosi, "Factors Affecting Software Developers Performance: An Integrated Approach," *Management Information Systems Quarterly*, Vol. 16, No. 3, 1992, pp. 395-413. doi:10.2307/249535

[16] J. E. Hunter and F. L. Schmidt, "Quantifying the Effects of Psychological Interventions on Employee Job Performance and Work Force Productivity," *American Psychologist*, Vol. 38, 1983, pp. 473-478. doi:10.1037/0003-066X.38.4.473

[17] A. A. Chesney and E. A. Locke, "Relationships Among Goal Difficulty Business Strategies and Performance on a Complex Management Simulation Task," *Academy of Management Review*, Vol. 34, No. 2, 1991, pp. 400-424. doi:10.2307/256448

[18] G. P. Latham and J. J. Baldes, "The 'Practical Significance' of Locke's Theory of Goal Setting," *Journal of Applied Psychology*, Vol. 60, No. 1, 1975, pp. 122-124. doi:10.1037/h0076354

[19] J. R. Terborg, "The Motivational Components of Goal Setting," *Journal of Applied Psychology*, Vol. 61, No. 5, 1976, pp. 613-621. doi:10.1037/0021-9010.61.5.613

[20] P. C. Earley, C. Lee and L. A. Hanson, "Joint Moderating Effects of Job Experience and Task Component Complexity: Relations Among Goal Setting, Task Strategies and Performance," *Journal of Organizational Behaviour*, Vol. 11, No. 1, 1990, pp. 3-15. doi:10.1002/job.4030110104

[21] P. C. Earley and B. C. Perry, "Work Plan Availability and Performance: An Assessment of Task Strategy Priming on Subsequent Task Completion," *Organizational Behaviour and Human Decision Processes*, Vol. 39, No. 3, 1987, pp. 279-302. doi:10.1016/0749-5978(87)90025-2

[22] P. C. Earley, G. B. Northcraft, C. Lee and T. R. Lituchy, "Impact of Process and Outcome Feedback on the Relation of Goal Setting to Task Performance," *Academy of Management Journal*, Vol. 33, No. 1, 1990, pp. 87-105. doi:10.2307/256353

[23] R. E. Wood and A. Bandura, "Social Cognitive Theory of Organizational Management," *Academy of Management Review*, Vol. 14, No. 3, 1989, pp. 361-384.

[24] P. C. Earley, P. Wojnaroski and W. Prest, "Task Planning and Energy Expended: Exploration of How Goals Influence Performance," *Journal of Applied Psychology*, Vol. 72, No. 1, 1987, pp. 107-114. doi:10.1037/0021-9010.72.1.107

[25] E. A. Locke and K. N. Shaw, "Atkinson's Inverse-Ucurve and the Missing Cognitive Variables," *Psychological Reports*, Vol. 55, 1984, pp. 403-414.

[26] G. E. Rejda, "Principles of Risk Management and Insurance," Addison-Wesley, New York, 1998.

[27] G. Hofstede, "Cultures and Organizations: Software of the Mind," Harper-Collins, London, 1994.

[28] T. M. Singelis, H. C. Triandis, D. S. Bhawuk and M.Gelfand, "Horizontal and Vertical Dimensions of Individualism and Collectivism: A Theoretical and Measurement Refinement," *Cross-Cultural Research*, Vol. 29, No. 3, 1995, pp. 240-275. doi:10.1177/106939719502900302

[29] H. C. Triandis, "Boulder", Westview Press, New York, 1995.

[30] N. W. Hui and H. C. Triandis, "Individualism-Collectivism: A Study of Cross-cultural Researchers," *Journal of Cross-Cultural Psychology*, Vol. 20, 1986, pp. 296-309.

[31] R. Lewicki and B. Burker, "Developing and Maintaining Trust in Work Relationships," Thousand Oaks, CA: Sage, 1996.

[32] R. Porta, F. Lopez-de-Silanes, A. Shleifer and R. Vishny, "Trust in Large Organizations," *Interaction of Economic*

Institutions and Theory, Vol. 87, No. 2, 1997, pp. 333-338. doi:10.1177/0022022189203004

[33] B. Misztal, "Trust in Modern Societies," Blackwell Publications, Malden, 1998.

[34] P. Ratnasingham, "Trust in Web Electronic Commerce Security," *Information Management and Computer Security*, Vol. 6, No. 4, 1998, pp. 162-166. doi:10.1108/09685229810227667

[35] J. Backhouse and G. Dhillon, "Structures of Responsibility and Security of Information Systems," *European Journal of Information Systems*, Vol. 5, 1996, pp. 2-9. doi:10.1057/ejis.1996.7

[36] R. Bener, "Risk Perception, Trust, and Credibility: A Case in Internet Banking," University College of London, London, 2000.

[37] J. Backhouse and G. Dhillon, "Electronic Thesauruses for Clinical Terms: A Methodological Approach," *Third European Conference in Information Systems*, Athens, Greece, 1995.

[38] S. Krimsky and O. Plough, "Environmental Haz ards: Communicating Risks as a Social Process," Auburn House, Maersk Alabama, 1988.

[39] G. P. Latham and E. A. Locke, "Self-regulation through goal setting," *Organizational Behaviour and Human Decision Processes*, Vol. 50, No. 2, 1991, pp. 212-47. doi:10.1016/0749-5978(91)90021-K

[40] J. Ansell and F. Wharton, "Risk: Analysis, Assessment and Management," John Wiley and Sons Ltd, West Sussex, 1992.

[41] P. Slovic, "Perception of Risk: Reflections on the Psychometric Paradigm in Social Theories of Risk," Green-Wood Publishing Group, 1992.

［42］A. Tversky and D. Kahneman, "Availability: A Heuristic for Judging Frequency and Probability," *Cognitive Psychology*, Vol. 10, 1973, pp. 34-52.

[43] "IT safe?" *CIO Magazine*, Vol. 12, No. 19, 1999.

[44] D. W. Straub and R. J. Welke, "Coping with Systems Risks: Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol. 22, No. 4, 1998, pp. 441-469. doi:10.2307/249551