# CONTROLLING INSIDER THREATS WITH INFORMATION SECURITY POLICIES

Yayla, Ali Alper, School of Management, PO Box 6000, Binghamton University-SUNY, Binghamton, NY, 13902, USA, ayayla@binghamton.edu

## Abstract

*Over the past decade, several studies, industry reports and surveys have revealed that insider threats constitute a significant role in information security. Following the literature, we categorized insider threats as intentional and unintentional. Computer misuse and fraud are considered as the two most common intentional threats, whereas, user errors and negligence are considered as the two most common unintentional threats. Building on the organizational behavior, psychology and criminology literatures, in this paper, we introduce different socio-behavioral control mechanisms to mitigate insider threats to information security. These mechanisms include employees' integration and commitment to their job and organization, deterrence measures, management of work related stress, awareness of security issues, and motivation of employees. These socio-behavioral mechanisms are also accompanied by technical aspects such as user interface of security tools and technology-based controls. Lastly, the integrative and reinforcing role of security policies within the proposed framework is discussed.*

*Keywords: Insider threat, Information security, Information security policy*

# 1 Introduction

As organizations are becoming more dependent on information technology, the emphasis on information security is getting more significant. Threats to information security have several dimensions including internal vs. external, human vs. non human, and accidental vs. intentional. While initially information security was seen as a technology problem that can be addressed via sophisticated hardware and software solutions, increasing number of security breaches proved that this is indeed mostly a people problem. That is, security is only as strong as the weakest link, and if technological controls are not recognized by users, systems will be compromised (Rudolph et al., 2002).

Several industry reports indicate that both intentional and unintentional insider threats are considered as one of the top ranked threats to information security over the past decade (Richardson, 2009). For instance, according to the 2004 E-crime Watch Survey (CSO, 2004), 36% of the respondents experienced unauthorized access by insiders. There is an increasing trend as the more recent survey reported that 49% of the respondents experienced malicious insider attacks (CSO, 2007). On the other hand, unintentional insider threats carry as much significance as intentional insider threats. The 2009 CSI Computer Crime and Security Survey revealed that about 66% of the respondents attributed at least some of their losses to non-malicious insiders, and 16% of the respondents claimed that all their losses were due to non-malicious insiders (Richardson, 2009).

New challenges that companies are facing today can be one of the reasons of increasing threats from non-malicious insiders. For instance, the popularity of social networking creates further problems for companies, since the line between what is company specific confidential information and what can be shareable at social networking sites is vague for most employees (Brenner, 2009). Even though companies started adopting policies to guide social networking behavior, assuring the effectiveness of these policies is another challenge as the 2010 Cisco Security Report revealed that 50% of the respondents admitted that they ignore company policies prohibiting the use of social media tools and 27% admitted that they change the settings of their corporate devices to access prohibited applications (Cisco, 2010). Another growing challenge for companies is the increased role of mobile devices such as smart phones, laptops and tablets, as 42% of the respondents to the 2009 CSI survey experienced theft of mobile hardware, which can be attributable to negligence of end-users (Richardson, 2009).

Considering both internal and external threats, several control mechanisms are embedded in organizations. However, as Higgins (1999) noted, “without a policy, security practices will be developed without clear demarcation of objectives and responsibilities, leading to increased weakness” (p.217). Considering the growing importance of insider threats, the main goal of this paper is to a) create a framework to reduce intentional and unintentional insider threats by investigating the underlying causes of these threats, and b) emphasize the reinforcing and integrative roles of information security policies to achieve effective control in organizations.

# 2 Intentional Insider Threats to Information Security

Schultz and Shumway (2001) defined insider attack as “the intentional misuse of computer systems by users who are authorized to access those systems and networks” (p.189). Parallel to this definition, we consider computer abuse and fraud as the most common intentional insider threats to information security. *Computer abuse* is the “unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information system by individuals” (Straub and Nance, 1990:47). Violations against hardware, programs, data and computer services are some of the possible computer abusing cases (Straub and Nance, 1990). On the other hand, reasons behind *computer fraud* cover a wide range from inadequate rewards and management control to lax enforcement of disciplinary rules (Bologna, 1993).

Deterrence is considered as one of the initial steps in preventing computer abuse and fraud. Effective deterrence requires organizations to consider the social psychology of fraud perpetrators and the control environment of the firm by utilizing mechanisms such as employee education, proactive fraud policies, use of analytical reviews, surprise audits, and adequate reporting programs (Bologna, 1993; 1997). Considering these point of views, in this section, we address computer fraud and abuse using three mechanisms: Integration and commitment of the employees to the organization, deterrence measures, and technology-based controls.

## 2.1 Integration and Commitment

In his discussion of social control by social bonds, Hirschi (1969) postulated that "delinquent acts result when an individual's bond to society is weak or broken" (p.6). This bond consists of attachment to others, commitment to conventional lines of action, involvement to conventional lines of activities, and belief in conventional values. Although the data for his study was collected from a youth survey, his approach to the Social Control Theory (SCT) found support at the organizational level. For instance, Hollinger (1986) reported that production and property deviance is more likely to occur when individual's attachment to an organization is low.

In their Integrated Strain-Control Paradigm theory, Elliott et al. (1979) divided Hirschi's SCT approach into two parts: integration and commitment. *Integration* (social or external bond) is the extent to which people are involved in and attached to conventional groups and institutions (Lilly et al., 2002). *Commitment,* on the other hand, is personal attachment to conventional roles, groups and institutions (Lilly et al., 2002). Parallel to this, Stanton et al. (2003) investigated the relation between organizational commitment and information security and reported that individuals with high organizational commitment are less likely to have behaviors that may put their company at risk.

Likewise, Lee et al. (2004) introduced the organizational trust context, which is defined in terms of attachment, commitment, involvement, and norms. They reported significant relationship between induction control intention (ICI) (i.e., intention to control another person's identification without authorization and illegally use software that can be accessed only by authorization) and involvement. However, their study failed to find support for the relationship between ICI and commitment.

Considering the essential role of integration and commitment, it would be logical to assume that intentional threats could be reduced by increasing employees' participation in organizational roles and morally bounding them using social norms. That is,

*Proposition 1: High levels of integration and commitment of employees to their organization will reduce intentional insider threats to information security.*

## 2.2 Deterrence Measures

Deterrent factors are considered passive administrative countermeasures, hence, their effectiveness depends completely on individuals (Straub and Welke, 1998). Awareness programs and policies/guidelines that specify proper use of computer systems are two of the most effective deterrence measures (Straub and Nance, 1990). Studies in the information systems (IS) literature found empirical support in favor of the effectiveness of deterrence measures (Kankanhalli et al., 2003; Lee et al., 2004). However, in order to be effective, deterrence measures should communicate disciplinary actions that will be exercised when perpetrators are identified (Blumstein, 1978). For instance, D'Arcy et al. (2009) reported that perceived certainty and perceived severity of sanctions have negative effect on IS misuse intentions.

Although organizations can choose from internal and external disciplinary actions, majority of the incidents are disciplined internally, and only few organizations report security incidents to external authorities (Straub, 1986; Straub and Nance, 1990). Out of various internal mechanisms, warnings and firings are the most exercised disciplinary actions followed by suspension and fines. However, several behavioral scientists discussed the “side effects” of punishment such as loss of trust, productivity, and loyalty (Skinner, 1953; Podsakoff et al. 1982). Therefore, to minimize these “side effects”, organizations should emphasize that misuse of computer systems is considered a criminal behavior and perpetrators will suffer from disciplinary actions to ensure that employees would consider the punishments as fair.

Deterrence measures reinforced with disciplinary actions will convince potential abusers that consequence of such an action is potentially bigger than its rewards. This point of view parallels the economic theory of punishment. This theory holds that people will avoid certain kinds of behavior if they find them infeasible or frightening (Siponen, 2000). Criminological theories, such as the Situational Crime Prevention and Rational Choice Perspective, also consider this reward/risk perspective. These considerations lead to our second proposition;

*Proposition 2: Deterrence measures that are reinforced with disciplinary actions will reduce intentional insider threats to information security.*

## 2.3 Technology-based Control

Technology-based controls can be used both for prevention and detection purposes (Straub, 1986; Baskerville, 1988). The aim of preventive control is towards reducing possible threats (Baskerville, 1988), mostly by controlling unauthorized access. Detective controls, on the other hand, are purposeful investigation of unauthorized activity, and based on examination of irregularities in system activities, as in the case of intrusion detection systems. Technology-based detective controls can be considered as the second line of defense after preventive controls, and they are designed to minimize the harm caused by threats by identifying security incident occurrences. In their study, Straub and Nance (1990) reported that around 50% of the detected computer abuses are discovered by system controls, and 16% of them discovered by purposeful investigation.

Some of the most common technology-based preventive and detective controls are passwords, firewalls, connection security, and cryptography (Haugen and Selin, 1999). Sandhu (2002) postulates that password based authentication is one of the persuasive technologies that can be implemented as a control mechanism. He further argues that although passwords are not as secure as biometric systems, they can be made strong enough for less critical processes. Similar to passwords, firewalls have become one of the most visible security technologies used in organizations (Brussin, 2002). Intrusion detection systems are also considered as effective detective controls since these tools are utilized not only to detect attacks but also to identify and analyze attack trends (Einwechter, 2002). Some of the more advanced computer-based controls that can be implemented are public key infrastructures, certificate authorities, and vulnerability assessment (Chokhani, 2002; Bace, 2002). The essential role of these control mechanisms leads to our third proposition;

*Proposition 3: Technology-based control mechanisms will reduce intentional insider threats to information security.*

# 3 Unintentional Insider Threats to Information Security

User errors and negligence are arguably the two most common unintentional insider threats. Whitman (2004) considers “act of human failures or error” as one of the most severe threats to information security. Some of the underlying reasons behind user errors are lack of experience in utilizing security tools, complexity of the security tools, and job stress due to time pressure and workload. On the other hand, although reasons behind negligence are complex, lack of awareness and motivation to use security tools due to their performance hindering characteristics can be considered as important factors. Thus, in this section, we propose to mitigate user error and negligence through five mechanisms: motivation, training, usability of security tools, time and workload pressure, and awareness.

## 3.1 Motivation

Several studies in the IS literature emphasized the positive effect of usefulness on technology acceptance (Davis et al., 1989; Taylor and Todd, 1995b). However, computer security tools are almost never considered from the performance enhancing perspective. In contrary, users consider computer security tools as performance restraining, since encrypting e-mails or managing secure passwords may require extra time, or using firewalls may slow down computer systems. In other words, within the context of security tools, extrinsic rewards of the behavior (e.g., performance increase) become relatively insignificant. Therefore, unless users are intrinsically motivated, successful adoption and usage of computer security tools is unlikely. Similar to these arguments, Boss et al. (2009) reported that apathy has negative effect on the level of precautions taken by users to secure their computers and adhere with security policies.

Intrinsically motivated behavior is a behavior that is aimed to satisfy individual’s needs for competence and self-determination (Deci, 1975). That is, people engage in intrinsically motivated activities considering internal consequences rather than an external reward. High levels of intrinsic motivation will also lead individuals to be more willing to use systems that require substantial amount of effort (Deci, 1975), which is commonly the case for the security tools. Inexperienced users, especially, would frequently fail to meet security requirements or to use security tools properly, and therefore, may never be intrinsically motivated towards implementing them properly in the future.

In the IS literature, *Computer Playfulness* is considered as an important intrinsic motivator. It refers to “individual’s tendency to interact spontaneously, inventively and imaginatively” with computers (Webster and Martocchio, 1992). It is important to note that we consider computer playfulness as a personal trait rather than a state (see Webster and Martocchio, 1992 and Woszczynski et al. 2002 for detailed comparison), and it is distinct from the enjoyment users would have as a result of interacting with computers. Studies reported significant indirect effects of computer playfulness on technology use through perceived ease of use (Venkatesh, 2000; Venkatesh et al., 2002) or through cognitive ability (Agarwal and Karahanna, 2000). Moreover, in the information security context, Bulgurcu et al. (2010) provided empirical support emphasizing the importance of intrinsic benefits and cost in terms of compliance with IS security policies. Therefore, we posit that high intrinsic motivation levels will increase usage of security tool, hence;

*Proposition 4: Increasing user’s intrinsic motivation will reduce unintentional insider threats to information security.*

## 3.2 Training

Training of employees is considered as one of the common methods to ensure their compliance with security policies (Puhakainen and Siponen, 2010). The positive effect of training to mitigate unintentional insider threats can be categorized in two groups. Firstly, training can increase users’ ability to interact with software programs (Nelson and Chenney, 1987). User skills are often considered as important determinants of intentions and behavior. For instance, a considerably stream of research based on the Theory of Planned Behavior (TPB) (Ajzen, 1988) investigated computer users’ intentions. The *Perceived Behavioral Control* (PBC) construct in TPB captures the perceived ease or difficulty of performing the behavior. Significant relationship has been reported in several empirical studies between PBC and intentions as well as between PBC and behavior (Taylor and Todd, 1995b). Especially for inexperienced users, PBC found to be an important determinant of intentions (Taylor and Todd, 1995a). Training towards enhancing individual’s skills is essential because system utilization and information acceptance are closely related with user abilities (Lee et al. 1995). Considering that end-users rarely possess adequate skills for computer security tools, the importance of training becomes even clearer.

Similarly, training can increase *Computer Self-efficacy*, and in turn, increase user performance and technology usage. Computer self-efficacy refers to individual's perceptions of his abilities to use computers to accomplish a specific task. Users are more likely to reject a computer system when their objective usability is lower than their computer self-efficacy. High levels of computer self-efficacy are essential since it is associated with better technology usage performance, especially when users are not familiar with software packages (Compeau and Higgins, 1995). Increased training not only affects post-training performance (Compeau and Higgins, 1995) but also affects post-training computer self-efficacy (Potosky, 2002). Moreover, studies showed that computer self efficacy has positive effect on the level of precautions taken by the users to secure their computers, use computer security software and adhere with information security policies (Herath and Rao, 2009; Boss et al., 2009).

Secondly, training can have a direct effect on technology usage. During training programs, user would have the opportunity to replicate instructor's behaviors and to engage in trial and error activities. The Social Learning Theory postulates that this direct experience will have positive influence on individual's learning process. Lippert and Forman (2005) operationalized this effect with their *Experimentation* construct and provided empirical support for the positive effect of experimentation on technology utilization. This direct experience users would gain from training will also have positive effects on individuals' intentions (Ajzen and Fishbein, 1980). Moreover, experience gained from training can be considered as a proxy to *Prior Experience*. Users with prior experience have stronger relationship between intentions and behavior than inexperienced users (Taylor and Todd, 1995b). For instance, prior experience with PCs can have a direct effect on utilization of PCs (Thompson et al., 1991).

An important conclusion can be drawn from these point of views. That is, even though users are rarely familiar with computer security tools, training will help them to improve their abilities, increase their computer self-efficacy and performance, and lastly increase their actual usage behavior. This leads to our fifth proposition;

*Proposition 5: Training users for security tools will reduce unintentional insider threats to information security.*

## 3.3 Usability of Security Tools

The effect of usability on unintentional insider threats is twofold. The first effect is in terms of users' intentions to use existing security tools. Intentions to use computer systems has long been investigated in the IS literature. The Technology Acceptance Model (TAM) (Davis, 1989) captures usability with the *Perceived Ease of Use* (PEOU) construct. It refers to "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989). PEOU has been empirically tested in many studies and reported as an important determinant of usefulness as well as users' attitudes especially when users are not very familiar with the systems (Davis, et al. 1989; Taylor and Todd 1995b). Similarly *Effort Expectancy*, which captures PEOU, complexity construct from Thompson et al.'s Model of PC Utilization (1991), and ease of use construct from Moore and Benbasat's (1991) adaptation of the Innovation Diffusion Theory, has positive effect on user's intentions to use a system (Venkatesh et al., 2003).

The second effect of usability on unintentional threats is in terms of preventing erroneous use in security technologies. This concept is introduced to IS literature by Saltzer and Schroeder (1975) as *Psychological Acceptability* (PA). PA is one of the eight specified design principles for constructing secure computer systems, and it focuses on designing human interfaces that are ease to use in order to prevent user errors. However, considerable amount of work reported that usability and security are hardly found together in computer systems, and security measures are difficult and confusing for an average computer user (Zurko and Simon, 1996; Whitten and Tygar, 1999). For example, easy to use passwords are not secure and secure passwords are not easy to use (Zurko and Simon, 1996). While erroneous use due to the difficulty of security programs can lead to severe security issues (Whitten and

Tygar, 1999), minor improvements to usability can result in significant progress in handling such tasks (Garfinkel and Miller, 2005). Therefore, it is logical to posit;

*Proposition 6: High levels of usability of security tools will reduce unintentional insider threats to information security.*

## 3.4 Time Pressure and Workload

Environmental conditions such as heavy and prolonged workload and constant time pressure are considered as major sources of stress and fatigue. The effect of emotional arouses on performance has first been investigated by Yerkes and Dudson (1908). Their well known inverted U-shaped relationship between arousal and performance was named as Y-D Law in psychology. This law postulates that both low and high arousal levels restrain performance. Later in the literature, this law has been utilized in several experimental studies by psychologists to investigate behavioral and cognitive consequences of such emotional arouses on individuals performance.

Although the definition of stress varies across research domains, some conditions that cause stress are generally accepted. Studies consistently reported that time pressure is a major source of stress (Bourne and Yaroush, 2003), and even well-trained individuals deviate from optimal behavior under time pressure (Lehner et al., 1997). Workload has also been considered as a source of stress. Individuals under heavy work demands (e.g. hard to reach goals) are threatened in two ways: losing their control over the work environment, and losing their rewards and be subject to punishment (Klein, 1971).

Heavy and prolonged workload can also cause fatigue. Experimental studies reported that fatigue has negative effects on even simple jobs such as data-entry (Buck-Gengler and Healy, 2001; Fendrich et al. 1995), and its effect increases with the complexity of the task (Soetens et al, 1992). Consequently, stress and fatigue, as low emotional arouses, restrain performance by increasing errors, reducing working memory and cue utilization (Bourne and Yaroush, 2003). This leads to our next proposition;

*Proposition 7: Reducing work related stress and fatigue levels by adjusting time pressure and workload will reduce unintentional insider threats to information security.*

## 3.5 Awareness

User negligence is a critical factor in the information security context. One way of fighting with negligence is creating awareness among users (Spurling, 1995; Thompson and von Solms, 1998). The awareness programs have two main objectives; a) making employees aware of procedures, rules and regulation stated in the security policy, and b) making employees aware of security concerns. Increasing users' awareness about security threats and computer-based controls such as authentications and antivirus systems will help them understand the severity of the threats and also increase utilization of these control mechanisms. However, given their importance, awareness programs constitute approximately 1% of security budgets in organizations (Richardson, 2009).

Rudolph et al. (2002) argue that "a staff that is aware of security concerns can prevent incidents" (p.29.2). They further discuss that employees can become detection instruments of the organization by getting familiar with danger signals through awareness programs. Moreover, awareness of employees can have positive effect on their beliefs and attitudes towards compliance with IS security policies as well as their perceived certainty and severity of sanctions (Bulgurcu et al., 2010; D'Arcy et al. 2009). These discussions lead to our last proposition;

*Proposition 8: Increasing user awareness will reduce unintentional insider threats to information security.*

# 4 The Role of Information Security Policies

One of the main objectives of information security policies is to provide a guideline and set of rules to the organization to prevent security breaches. A good security policy should "outline individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee reporting of identified or suspected threats to the system, define penalties for violations, and provide a mechanism for updating the policy" (Whitman, 2004: 52). The focus of any security should be to "create a shared vision and an understanding of how various controls will be used such that the data and information is protected" (Dhillion, 1999). In other words, security policies need to communicate potential risks and risk mitigation methods that are in place to users as well as to top management.

Within the context of insider threats, the first role of security policies is to act as a reinforcing mechanism so that the factors outlined above are considered at the decision making level as well as at the user level. For instance, training and awareness programs tend to be one of the first places top management looks when budget cuts are necessary (Schultz, 2004). Security policies should be governing enough to prevent these programs from being terminated. Another example is the role of security policies in an employee's job definition. In this case, security policies should be reinforcing enough to prevent employees from being under a lot of work related stress. From the user's perspective, this is similar to Boss et al.'s (2009) concept of "mandatoriness", where the level of precautions taken by the user increases as with her perceived mandatoriness of the information security policies.

However, the existence of policies does not guarantee that users have read them or they are aware of their content. Foltz et al. (2005) demonstrated this issue using students and security policies in a university. They revealed that although it wasn't enough to influence all subjects, even one time exposure to such policies increased the awareness of the students. Likewise, in an organization setting, policies are exposed to employees very few times, mostly during the hiring process. Therefore, it would not be surprising to see similar results in organizations as well. According to von Solms and von Solms (2004), to ensure that employees follow sentiments of the management stated in policies, an appropriate group culture needs to be cultivated. Moreover, to ensure acceptable behaviors from employees, this culture has to be synchronized by underlying policies.

Policies that are part of the organizational culture would be beneficiary for the organization to make sure that employees are not only aware of these policies but also willing to use these policies as guidelines for appropriate behavior. However, information security policies are mostly stand-alone policies initiated by the IT departments with limited governing power. One potentially effective method to increase the effect of such policies is to integrate them to the existing non-IT policies in the organization (e.g., corporate policy, personnel policy). This integration will increase the effectiveness of security policies and make them part of the organizational culture. Findings supporting this view were reported by Puhakainen and Siponen (2010) in terms of integrating IS security training with normal business communication to prevent employees from perceiving IS security as a separate issue. Another example is the integration of human resources policies and security policies to ensure that hiring, termination and layoff procedures do not conflict with security requirements. More specifically, procedures for firing an employee should be synchronized effectively without creating any opportunity for further threat. This is parallel to Cohen and Felson's (1979) Routine Activity Theory, which posits that "the key to stopping crime is to prevent the intersection in time and space of offenders and of targets that lack guardianship" (Lilly et al., 2002).

In summary, in order to ensure effective control, information security policies should have two important characteristics: reinforcing and integrative. The reinforcing role captures the essential goal of minimizing insider threats by drawing attention to the discussed factors. The integrative role prevents these policies from being stand-alone procedures and incorporates them into organization's existing culture. Figure 1 summarizes our discussions and depicts the two important roles of information security policies to achieve effective control of insider threats.

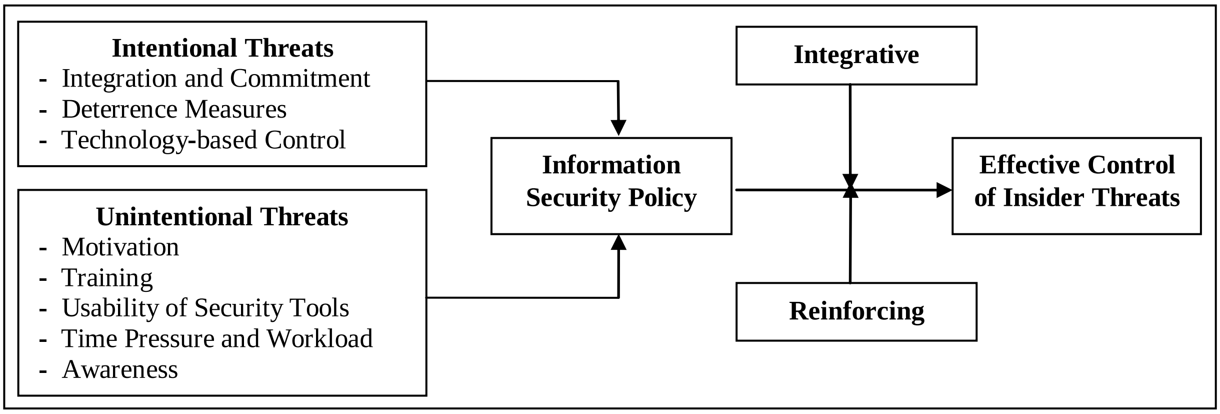
Intentional Threats
- Integration and Commitment
- Deterrence Measures
- Technology-based Control
Unintentional Threats
- Motivation
- Training
- Usability of Security Tools
- Time Pressure and Workload
- Awareness
Information Security Policy
Integrative
Reinforcing
Effective Control of Insider Threats

*Figure 1. The proposed framework for controlling insider threats to information security.*

## 5 Discussion

This paper introduces a framework that is aimed to control insider threats to information security. Following the literature, insider threats are categorized as intentional and unintentional. In order to mitigate intentional insider threats, the proposed framework draws connections to the organizational behavior, criminology and psychology literatures. Increasing employee integration and commitment, using deterrent measures, and finally implementing technology-based controls are proposed as potential measures to control intentional threats.

On the other hand, unintentional threats can be controlled or mitigated by increasing employees' intrinsic motivation, providing training for security tools, implementing security tools with high level of usability, adjusting time pressure and workload on employees, and finally by increasing awareness among users and management.

Socio-behavioral side of insider threats, although studied extensively, is neglected in the security policy context. Security policies are mostly associated with physical security, network security, and Internet and e-mail security (Barman, 2002; Kabay, 2002). However, these policies should also incorporate different behavioral and psychological aspects (attachment, involvement, punishment, job stress, etc.) as captured in our framework. Therefore, we make an important contribution by pointing out that security policies need to be reinforcing while considering this socio-behavioral side of insider threats. Moreover, we emphasize the importance of integration of the control mechanisms to the organizational culture through security policies.

One of the limitations of the paper comes from the conceptualization of insiders only as the employees of an organization. However, contractors, consultants, company partners and suppliers may also have access to raise insider threats. Another limitation, which is also emphasized by D'Arcy and Hovav (2004), is that the individual characteristics of users (e.g., gender, age and risk propensity) are not considered in the framework. These characteristics can moderate the effects of discussed factors. Future research should focus on empirical testing of the proposed framework and also expanding the proposed framework by incorporating external threats and non-human threats to information security such as hackers, natural disasters and systems failures.

## References

Agarwal, R. and Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. MIS Quarterly, 24(4), 665-694.

Ajzen, I. (1988). Attitudes, Personality and Behavior. Chicago: Dorsey Press.

Ajzen, I. and Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior. Englewood Cliffs, NJ: Prentice-Hall Inc.

Bace, R.G. (2002). Vulnerability assessment and intrusion detection systems. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley & Sons, Inc.

Barman, S. (2002). Writing Information Security Policies. Indianapolis: New Riders.

Baskerville, R. (1988). Designing Information Systems Security. New York, NY: John Wiley Information Series.

Blumstein, A. (1978). Introduction. In A. Blumstein, J. Cohen and D. Nagin (Eds.), Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates. Washington, DC: National Academy of Sciences.

Bologna, J. (1993). Handbook of Corporate Fraud. Boston, MA: Butterworth-Heinemann.

Bourne, L.E. and Yaroush, R. (2003). Stress and cognition: A cognitive psychological perspective. Unpublished paper.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2010). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18, 151-164.

Brenner, B. (2009). The Global Information Security Survey. CXO Media Inc.

Brussin, D. (2002). Firewall and proxy servers. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley & Sons, Inc.

Buck-Gengler, C.J. and Healy, A.F. (2001). Processes underlying long-term repetition priming in digit data entry. Journal of Experimental Psychology: Learning, Memory, and Cognition, 27, 879-888.

Bulgurcu, B, Cavusoglu, H. and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.

Chokhani, S. (2002). Public Key Infrastructures and Certificate Authorities. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook.

Cisco. (2010). Cisco 2010 Midyear Security Report. Cisco Systems, Inc.

Cohen, A.K. and Felson, M. (1979). Social change and crime rate trends: A routine activities approach. American Sociological Review, 44, 588-608.

Compeau, D.R. and Higgins, C.A. (1995). Application of Social Cognitive Theory to training for computer skills. Information Systems Research, 6(2), 118-143.

CSO Magazine. (2004). E-Crime Watch Survey, CXO Media Inc.

CSO Magazine. (2007). E-Crime Watch Survey, CXO Media Inc.

D'Arcy, J. and Hovav, A. (2004). The role of individual characteristics on the effectiveness of IS security countermeasures. In Proceedings of the Tenth AMCIS, New York, NY.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.

Davis, F.D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13: 319-339.

Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. (1989). User acceptance of computer technology: A comparison of two theoretical models. Management Science, 35, 982-1003.

Deci, E.L. (1975). Intrinsic Motivation. New York, NY: Plenum Press.

Dhillon, G. (1999). Managing and controlling computer misuse. Information Management & Computer Security, 7(4), 171.

Einwechter, N. (2002). Preventing and detecting insider attacks using IDS, Online document at: http://online.securityfocus.com/infocus/1558.

Elliott, D.S., Ageton, S.S. and Canter, R.J. (1979). An integrated theoretical perspective on delinquent behavior. Journal of Research on Crime and Delinquency, 16, 3-27.

Fendrich, D.W., Healy, A.F. and Bourne, L.E. (1991). Long-term repetition effects for motoric and perceptual procedures. Journal of Experimental Psychology: Learning, Memory, and Cognition, 17, 137-151.

Foltz, C.B., Cronan, T.P. and Jones, T.W. (2005). Have you met your organization's computer usage policy? Information Management & Data Systems, 105(2), 137-146.

Garfinkel, S.L. and Miller, R.C. (2005). Johnny 2: A user test of key continuity management with S/MIME and Outlook Express. Working paper.

Haugen, S. and Selin, J.R. (1999). Identifying and controlling computer crime and employee fraud. Industrial Management & Data Systems, 99(8), 340-344.

Herath, T. and Rao, H.R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems, 18, 106-125.

Higgins, N.H. (1999). Corporate system security: towards an integrated management approach. Information Management & Computer Security, 7(5), 217-222.

Hirschi, T. (1969). Causes of Delinquency. Berkeley: University of California Press.

Hollinger, R.C. (1986). Acts against the workplace: Social bonding and employee deviance. Deviant Behavior, 7, 53-75.

Kabay, M.E. (2002). Developing security policies. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley & Sons, Inc.

Kankanhalli, A., Teo, H., Tan, B.C.Y. and Wei, K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23, 139-154.

Klein, S.M. (1971). Workers under stress. Lexington: University Press of Kentucky.

Lee, S.M., Kim, Y.R. and Lee, J. (1995). An empirical study of the relationships among end user information systems acceptance, training, and effectiveness. Journal of Management Information Systems, 12(2), 189-202.

Lee, S.M., Lee, S. and Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41, 707-718.

Lehner, P., Seyed-Solorforough, M., O'Connor, M.F., Sak, S. and Mullin, T. (1997). Cognitive biases and time stress in team decision making. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems & Humans, 27, 698-703.

Lilly, J.R., Cullen, F.T. and Ball, R.A. (2002). Criminological Theory: Context and Consequences. Thousand Oaks: Sage Publications.

Lippert, S.K. and Forman, H. (2005). Utilization of information technology: Examining cognitive and experiential actors of post-adoption behavior. IEEE Transactions on Engineering Management, 52, 363-381.

Moore, G.C. and Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. Information Systems Research, 2(3), 192-222.

Nelson, R.R. and Cheney, P.H. (1987). Training end users: Exploratory study. MIS Quarterly, 11(4), 547-559.

Podsakoff, P.M., Todor, W.D. and Skov, R. (1982). Effects of leader contingent and noncontingent rewards and punishment behaviors on subordinate performance and satisfaction. Academy of Management Journal, 25(4), 810-821.

Potosky, D. (2002). A field study of computer efficacy beliefs as an outcome of training: the role of computer playfulness, computer knowledge, and performance during training. Computers in Human Behavior, 18, 241-255.

Puhakainen, P. and Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757-778.

Richardson, R. (2009). CSI Computer Crime & Security Survey. Computer Security Institute.

Rudolph, K., Warshawsky, G. and Numkin, L. (2002). Security Awareness. In S. Bosworth and M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley & Sons, Inc.

Saltzer, J.H. and Schroeder, M.D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(1).

Sandhu, R. (2002). Identification and Authentication. In S. Bosworth & M. E. Kabay (Eds.), Computer Security Handbook, 4th ed. New York: John Wiley & Sons, Inc.

Schultz, E.E. (2004). Security training and awareness-fitting a square peg in a round hole. Computer & Security, 23, 1-2.

Schultz, E.E. and Shumway, R. (2001). Incident Response: A Strategic Guide for System and Network Security Breaches. Indianapolis, IN: New Riders.

Siponen, M.T. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. Information Management & Computer Security, 8(5), 197-209.

Skinner, B.F. (1953). Science and Human Behavior. New York: Macmillan.

Soetens, E., Hueting, J. and Wauters, F. (1992). Traces of fatigue in an attention task. Bulletin of the Psychonomic Society, 30, 97-100.

Spurling, P. (1995). Promoting security awareness and commitment. Information Management and Computer Security, 3(2), 20-26.

Stanton, M.S., Stam, K.R., Guzman, I. and Caldera, C. (2003). Examining the linkage between organizational commitment and information security. Paper presented at the Proceedings of the IEEE Systems, Man, and Cybernetics Conference, Washington, DC.

Straub, D.W. (1986). Computer abuse and computer security: Update on an empirical study. Security, Audit, and Control Review, ACM Special Interest Group Journal, 4(2), 21-31.

Straub, D.W. and Nance, W.D. (1990). Discovering and disciplining computer abuse in organization. MIS Quarterly, 14(1), 45-60.

Straub, D.W. and Welke, J.R. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 22(4), 441.

Taylor, S. and Todd, P.A. (1995a). Assessing IT usage: The role of prior experience. MIS Quarterly, 19(4): 561-570.

Taylor, S. and Todd, P.A. (1995b). Understanding information technology usage: A test of competing models. Information Systems Research, 6(2), 144-176.

Thompson, M.E. and von Solms, B. (1998). Information security awareness: educating our users effectively. Information Management & Computer Security, 6(4), 167-173.

Thompson, R. L., Higgins, C. A., & Howell, J. M. 1991. Personal computing: Toward a conceptual model of utilization. MIS Quarterly, 15(1), 124-143.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the Technology Acceptance Model. Information Systems Research, 11(4) 342-365.

Venkatesh, V., Morris, M., Davis, G.B. and Davis, F.D. (2003). User acceptance of Information Technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.

Venkatesh, V., Speier, C. and Morris, M.G. (2002). User acceptance enablers in individual decision making about technology: Toward and integrated model. Decision Sciences, 33(2), 297-316.

von Solms, R. and von Solms, B. (2004). From policies to culture. Computers & Security, 23, 275-279.

Webster, J. and Martocchio, J.J. (1992). Microcomputer playfulness: Development of a measure with workplace implication. MIS Quarterly, 16(2), 201-226.

Whitman, M.E. (2004). In defense of the realm: Understanding the threats to information security. International Journal of Information Management, 24, 43-57.

Whitten, A. and Tygar, J.D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Paper presented at the Proceedings of the 8th USENIX Security Symposium, Washington, DC.

Woszczynski, A.B., Roth, P.L. and Seagers, A.H. (2002). Exploring the theoretical foundations of playfulness in computer interactions. Computers in Human Behavior, 18, 369-388.

Yerkes, R.M. and Dodson, J.D. (1908). The relation of strength of stimulus to rapidity of habit-formation. Journal of Comparative Neurology and Psychology, 18, 459-482.

Zurko, M.E. and Simon, R.T. (1996). User-centered security. The ACM New Security Paradigms Workshop, Lake Arrowhead, CA.