Computers & Security (2005) **24**, 472—484

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

The insider threat to information systems and the effectiveness of ISO17799

Marianthi Theoharidou [a], Spyros Kokolakis [b,*], Maria Karyda [a], Evangelos Kiountouzis [a]

[a] *Department of Informatics, Athens University of Economics and Business, 76 Patission Ave., Athens GR-10434, Greece*
[b] *Department of Information & Communication Systems Engineering, University of the Aegean, Karlovassi, Samos GR-83200, Greece*

Received 7 June 2004; revised 4 April 2005; accepted 10 May 2005

KEYWORDS
Insider threat;
Computer misuse;
IS security management;
Criminology theories;
ISO17799

Abstract Insider threat is widely recognised as an issue of utmost importance for IS security management. In this paper, we investigate the approach followed by ISO17799, the dominant standard in IS security management, in addressing this type of threat. We unfold the criminology theory that has designated the measures against insider misuse suggested by the standard, i.e. the General Deterrence Theory, and explore the possible enhancements to the standard that could result from the study of more recent criminology theories. The paper concludes with supporting the argument for a multiparadigm and multidisciplinary approach towards IS security management and insider threat mitigation.

Introduction

Until quite recently the view of Information Systems (IS) security as a technical issue has dominated IS security research and practice. Lately, a new paradigm is emerging, addressing it as a ''people issue'' and an ''organisation issue'' (Hinde, 2003). Under this perspective, the importance of IS security management in the organisational context has become evident and modern organisations strive to establish effective security management practices. Nevertheless, this task is challenging due to the multitude of factors involved and the inherent unpredictability of human behaviour.

Since the International Organisation for Standardisation (ISO) adopted the British Standard BS7799 (''Code of practice for information security management'') and published it as an International Standard (ISO/IEC, 2000), an increasing volume of organisations world-wide have organised their IS

* Corresponding author.
E-mail addresses: mtheohar@aueb.gr (M. Theoharidou), sak@aegean.gr (S. Kokolakis), mka@aueb.gr (M. Karyda), eak@aueb.gr (E. Kiountouzis).

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.05.002

security management system on the basis of this standard (referred in the rest of the paper as ISO17799). So far, more than 1300 organisations have been certified under the ISO17799 standard (see http://www.xisec.com/register.htm) and many more are in the process, which makes it one of the most popular standards for IS security management.

ISO17799 provides a set of recommendations for information security management. Its focus is on the protection of information as an asset, nevertheless it adopts a broad perspective that covers most aspects of IS security (e.g. physical security, personnel security etc.). At this point we should clarify the meaning of the two terms. *Information security* refers to the preservation of confidentiality, integrity and availability of information (ISO/IEC, 2000). Respectively, *IS security* refers to the protection of all elements constituting an IS (i.e. hardware, software, information, people and processes). Therefore, IS security is a broader term that can be used for accommodating information security as well.

Information security management in ISO17799 is based on risk management. The latter is defined in the standard as the ''[p]rocess of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost'' (ISO/IEC, 2000). Risk mitigation is achieved, mainly, through the implementation of appropriate controls, which address a wide range of threats.

Modern information systems are confronted by a variety of threats. Although attacks originating from outside, such as hacking attempts or viruses, have gained a lot of publicity, insider threats pose a significantly greater level of risk (Schultz, 2002). Unfortunately, the controls and tools that are used for the protection of the IS from externally initiated attacks (e.g. firewalls and intrusion detection systems) are not effective in detaining insider threat, as the latter requires a different approach (Porter, 2003; Lee and Lee, 2002; Schultz, 2002).

Considering the popularity of the standard and its influence on the IS security management practice, the authors believe that it is significant to identify the deficiencies of the standard and to suggest improvements, especially in a very intriguing issue such as the insider threat. This paper aims to provide a critical analysis of the approach adopted by ISO17799 in addressing insider threat. The following section provides an overview of the insider threat issue and how it is addressed in the field of IS security. It also includes an extended description of criminology theories that can be applied in the study of computer abuse within organisations. The third section presents a critical analysis of ISO17799 with respect to the issues addressed by criminology theories and the means proposed in the standard for tackling them. In the fourth section, implications of the analysis and suggestions for enhancing security management practice are presented. The last section summarises our thesis and indicates areas for further research.

The insider threat and criminology theories

Insider misuse of information systems is a form of delinquent behaviour in the workplace. Criminology research has extensively studied this kind of behaviour, despite the fact that it does not always lead to committing a crime. In this section we present previous research work on insider threat, as well as the major criminology theories and their implications for IS security management.

The insider threat

In this paper the term *insider threat* refers to threats originating from people who have been given access rights to an IS and misuse their privileges, thus violating the IS security policy of the organisation.

Relative research has focused on categorising, modelling, detecting and addressing insider threat. Neumann (1999) categorises insiders according to their type of access (i.e. logical vs. physical, ordinary vs. privileged). The US National Security Telecommunications and Information Systems Security Committee (NSTISSAM, 1999) distinguishes four categories (namely traitor, zealot, browser, and well-intentioned) of insiders, depending on their aims. A more recent study (Stanton et al., 2005) provides a six-element taxonomy of security behaviour (intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance, basic hygiene), using intentionality and technical expertise as criteria. Finally, Tuglular (2000) provides a list of characteristics for the classification of internally initiated security incidents.

Other researchers have proposed models that enable analysing and understanding the insider misuse phenomenon. A much-cited model described in (Wood, 2000) defines three prerequisites for an insider to mount an attack, i.e. *capability*, *motive*, and *opportunity*. A similar model introduced by Parker (1998) defines five factors (i.e. *skills*, *knowledge*, *resources*, *authority*, and *motive*). Dhillon and Moores (2001) also suggest that computer crime committed by current employees is a rational act and a result of *personal factors*, *work situations* and *available opportunities*.

Schultz (2002) defines a set of cues that may indicate that an insider attack is imminent (i.e. deliberate markers, meaningful errors, preparatory behaviour, correlated use patterns, verbal behaviour, personality traits). Magklaras and Furnell (in press) focus on the *capability* and *opportunity* factors and propose a model of end user sophistication, which could be embedded in an insider threat prediction tool.

Knowledge and use of these tools and models can prove effective in detecting and analysing insider misuse. However, protecting a system from the insider threat also involves deterrence, prevention and containment of misuse. Therefore, research on this issue has been based on theories originated from the field of criminology. In the following paragraphs we briefly present some of the most influential criminology theories and show how these apply to studying the insider threat.

The impact of criminology theories on IS security management

The analysis of the literature on insider threat has showed that the tools and methods applied have their roots in criminology, since concepts such as 'computer crime', 'computer abuse/misuse', 'deterrence', 'motives' and so on are widely used (see Hollinger, 1993; Neumann, 1999; Parker, 1998; Tuglular, 2000; Willison, 2004). In the next section we analyze major theoretical approaches employed in criminology, as we believe that by studying the theoretical origin of the tools and methods, we can derive useful conclusions as to the possible reasons for their lack of effectiveness and indications for their improvement.

General Deterrence Theory

General Deterrence Theory (GDT) has been widely used in the study of criminal and antisocial behaviour and is a well-established theory within the criminology field. It is based on the hypothesis that people make logical decisions based on the maximization of their benefit and the minimization of cost (Beccaria, 1963). It focuses on the '*disincentives*' or *sanctions* against committing a criminal act and their effectiveness as a deterrent. Blumstein (1978) suggests that the effectiveness of such disincentives is based on: (a) certainty of sanction and (b) severity of sanction (Straub and Welke, 1998).

This theory suggests that when the possibility of punishment is high and the sanction is severe, potential criminals will be deterred from committing illegal acts, especially when their motives are weak. If we consider insider abuse as typical, white-collar crime, it takes place in a rather benevolent environment, by people who usually conform to rules and regulations. In this context, sanctions are believed to be effective because, though employees may desire to break the social norms in order to benefit, their motives are weak and, therefore, deterrence mechanisms can prove effective (Straub, 1990).

GDT is also well established within the IS security field (Straub, 1990; Straub and Welke, 1998) and has been applied in order to deter computer abuse. One instance of its application is the *Security Action Cycle* (Straub and Welke, 1998). According to this model, computer abuse must be handled at four stages:

1. *Deterrence*. Most of the potential offenders are deterred through mechanisms such as policies, guidelines, and awareness programmes.
2. *Prevention*. If deterrence proves to be ineffective, prevention mechanisms are used, such as physical or procedural controls.
3. *Detection*. The mechanisms at this stage address the realisation of computer abuse, aiming to make such abuses known.
4. *Remedies*. When a computer abuse act is detected, its consequences should be treated and actions against the offender should be taken, according to the organisation's policy and rules.

This model identifies the aim of IS security management as the maximization of the number of deterred and prevented abusive acts and the minimization of the number of detected and punished ones. It also uses a feedback mechanism, as depicted in Fig. 1, through which the deterrence stage is informed by the next three stages, in order to make potential offenders aware of the consequences involved in committing abusive acts.

Parker (1998) employs the core concepts from the Security Action Cycle for the theoretical grounding of the security framework he proposes; his model sets the following security goals: *avoidance*, *deterrence*, *prevention*, *detection*, *mitigation*, *sanction*, *transference*, *investigation*, *recovery and correction*. Another example is a recent report on mitigating the insider threat, published by the

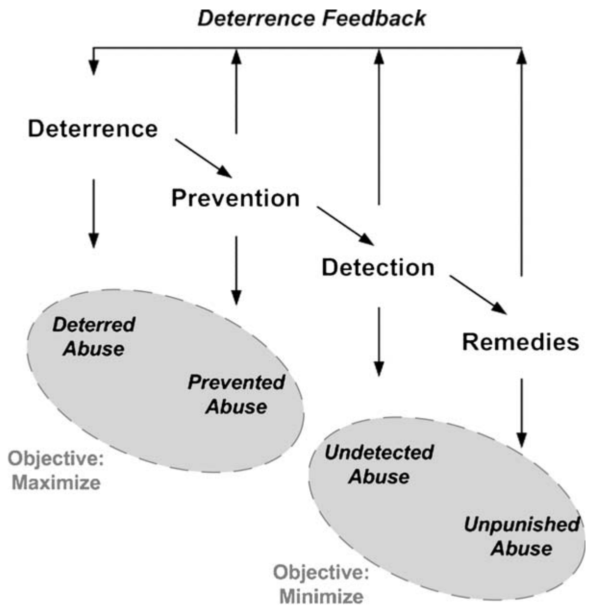

Figure 1 The Security Action Cycle (based on Straub and Welke (1998)).

US Department of Defense Information Systems (DoD-ITIPT, 2000). It contains a set of recommendations addressing the insider threat, emphasising on employees' awareness and accountability which are pursued by the use of personnel policies, and deterrence that can be achieved ''...*by publicizing the consequences of misuse, abuse and malicious activity and the operational use of measures to detect those behaviours*''.

Social Bond Theory

Social Bond Theory (SBT) is a popular theory in criminology, which seeks to explain social behaviour that does not conform to generally accepted social rules. It is based on the hypothesis that despite a person's natural inclination towards crime, strong *social bonds* deter him/her from committing criminal acts. Under this assumption, the possibility of a person being involved in a crime increases when social bonds become weaker.

Hirschi (1969) defines four types of social bonds that promote socialization and conformity:

(a) *Attachment* refers to a person's interest in his/her social surroundings. The level of acceptance of social norms and the development of social consciousness depend on the attachment of an individual to other human beings. Most important social institutions include family, school and peers.
(b) *Commitment* to socially accepted goals is based on the notion that people who invest time, energy and effort in achieving social status, education, property or reputation are less likely to engage in criminal acts that may jeopardize their achievements.
(c) *Involvement* in conventional activities, like school, family, work or recreation, leaves little time available for a person to engage in criminal acts.
(d) Finally, when *beliefs* in social values are absent or weak, the possibility of a person engaging in antisocial acts increases.

Lee and Lee (2002) explore the effectiveness of the SBT theory with regard to computer crime in organisations. Their findings reveal the important role that social bonds play in deterring potential criminal acts. Agnew (1995), as described in Lee and Lee (2002), has also explored the application of the SBT with regard to IS security, and concludes that the positive perception of a crime can direct a person to committing criminal actions despite the high risk of punishment. Furthermore, Hollinger's research, as referred to in Vardi and Wiener (1996), indicates that employees are more likely to engage in criminal acts when their attachment to the organisation is weak (Hollinger, 1986).

A more recent study by Lee et al. (2003) tests the effectiveness of a combined model of GDT and SBT for addressing the IS insider threat. This study explores whether factors belonging to the GDT (such as security policy, security system, awareness programmes) can reduce computer abuse in general and whether factors related to organisational trust (the four social bonds of attachment, commitment, involvement and belief) can reduce computer abuse by employees. It shows that the bond of involvement (participation in informal meetings, personal relationships with many people, loyalty to the company) proves to be effective and that the belief that computer abuse is unacceptable reduces computer abuse by employees.

Social Learning Theory

Social Learning Theory (SLT) is based on Sutherland's theory of *differential association* (Sutherland, 1924) and Akers' theory of *Differential reinforcement/punishment* (Akers, 1977). According to this theory, as Lee and Lee (2002) have elaborated, a person commits a crime because (s)he has been associated with delinquent peers, who transmit delinquent ideas, reinforce delinquency, and function as delinquent role models.

There are four conceptual constructs used in this theory for explaining the potential effect that the social surrounding can have on an individual, with regard to engaging in criminal behaviour:

(a) *Differential association*: it is the process during which a person is exposed to normative definitions that favour or are against criminal behaviour.
(b) *Differential reinforcement/punishment*: it refers to the balance of expected or realized reward and punishment resulting from criminal behaviour.
(c) *Definition of behaviour*: the rationalization of a behaviour as good or bad, right or wrong, desirable or not, justified or not.
(d) *Imitation*: the engagement in behaviour after observing similar behaviour by others.

Lee and Lee (2002) discuss the results of various research approaches, with regard to the effectiveness of applying the SLT in IS security management. The theoretical model they propose suggests that employees are influenced by coworkers and seniors. The application of the SLT in IS security management is also supported by Skinner and Fream (1997), who found that differential association, differential reinforcement, definitions and imitation significantly influence computer abuse, as well as by Hollinger (1993), who points out the existence of a strong positive correlation between an individual engaging in computer abuse and the involvement of his/her friends in similar acts.

Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) (Ajzen and Fishbein, 1980) is considered as one of the most influential and popular conceptual frameworks for the study of human action (Ajzen, 2002). This theory attempts to explain the causal relation underlying human behaviour. The basic assumption is that a person's intention is a key factor for predicting a person's behaviour. *Intentions* are shaped by a series of factors that are explained in the following:

(a) *Attitude* towards behaviour. This factor describes the degree a person favours or not a certain behaviour. If (s)he perceives the result of a behaviour as positive, then (s)he shapes a positive attitude towards it; in the opposite case (s)he forms a negative attitude.
(b) Social factors called *subjective norms*. The social surroundings exercise pressure on individuals for or against adopting a certain behaviour. In other words a person becomes aware of normative beliefs concerning a behaviour. In order to adopt the behaviour, (s)he must first be motivated to comply with social demands. If the social surroundings consider a certain behaviour as positive and the person seeks social approval, then (s)he will adopt a positive subjective norm. If the behaviour is considered negative and the person is motivated to comply with his/her social surroundings, then (s)he is expected to adopt a negative subjective norm.
(c) Control factors which are characterized by the term *perceived behavioural control*. A person shapes intentions with regard to a behaviour based on his/her personal beliefs concerning: (a) the difficulty of realizing the behaviour and (b) his/her ability in successfully carrying it. If (s)he believes that there are factors that help or inhibit the adoption of a behaviour, (s)he will, respectively, have strong or weak perceived behavioural control. This last factor is crucial because even if the person has a positive attitude and subjective norm, (s)he will not adopt the behaviour unless (s)he has strong perceived control over it.

Finally, given a sufficient degree of *actual control* over the behaviour, people are expected to realize their intentions when the opportunity arises. Intention is thus assumed to be the immediate antecedent of behaviour. However, behaviours often pose difficulties of execution that may limit volitional control; it is useful to consider perceived behavioural control in addition to intention. To the extent that people are realistic in their judgments of a behaviour's difficulty, a measure of perceived behavioural control can serve as a proxy for actual control and contribute to the prediction of the behaviour in question (Ajzen, 2002).

The application of the Theory of Planned Behaviour with regard to acts of computer abuse is explored by Lee and Lee (2002), in combination with the first three theories we analyzed. Specifically, they suggest that *social bonds* affect the attitude of a person towards behaviour, *social learning factors* affect the subjective norms a person adopts and that *general deterrence factors* form perceived behavioural control.

The core concepts of this theory and particularly the concept of subjective norms can also be found in Leach's work about improving user security behaviour (Leach, 2003). Leach suggests that users' behaviour is affected by their understanding of what behaviour is expected by the employees, as well as by their willingness to comply with accepted norms. Key factors are the behaviour demonstrated by senior management and colleagues and the users' psychological contract with their employer, meaning the sense of obligation towards their employer.

Situational Crime Prevention

The theory of Situational Crime Prevention (SCP) (Clarke, 1980) is based on the hypothesis that to commit a crime, a person must have both *motive* and *opportunity*. It differs from the other theories, in the sense that it is not concerned with the formation of motives; instead it aims to reduce available opportunities, which are necessary for the realisation of criminal acts.

This theory is based on the principles of the *routine activity theory* and the *rational choice theory*. Routine activity theory (Clarke, 1980; Willison, 2001, 2004) focuses on the characteristics of the crime and not on the person committing the criminal act; it explores the mechanism through which social changes in the numbers of 'suitable targets' for a crime, or in the numbers of 'capable guardians' against crime can increase or reduce a crime rate. The rational choice perspective (Clarke, 1980), on the other hand, tries to explain crime from the perspective of the offender. It focuses on the thinking process of an offender, how (s)he evaluates criminal opportunities and how (s)he reaches the decision of committing a crime or not.

The theory of Situational Crime Prevention uses these concepts and aims to the undertaking of measures that will reduce the criminal opportunities in a certain context where criminal actions take place. These measures address issues concerning the formation, management or change of the environment and their goal is:

(a) To make a criminal act appear *more difficult*, by requiring increased effort (target hardening, access control, deflecting offenders, controlling facilitators).
(b) To make a criminal act appear *more dangerous*, meaning that it can be detected (entry/exit screening, surveillance — formal, natural or surveillance by employees).
(c) To *reduce the benefit* a person is expecting to receive (target removal, identifying property, reducing temptation, denying benefits).
(d) To *remove the excuses* a person can make in order to justify his/her actions (rule setting, stimulating conscience, controlling disinhibitors, facilitating compliance).

Willison (2001, 2004) suggests that the theory of Situational Crime Prevention and its core concepts can be applied in the IS security management field, providing a theoretical basis for understanding and addressing the issue of computer abuse within organisations.

Synopsis

Criminology theories provide the theoretical foundation for several models and strategies, which are currently widely employed for addressing the insider threat. Key theoretical concepts pertaining to the application of security controls aiming to combat insider abuse can be traced back to these theories, as the analysis presented earlier has shown. In this way, theories on criminal behaviour can be employed in the context of IS security management, providing directions as well as indications for the means to be used in the attempt to address the insider threat. These theories can be categorized according to their focal concept and their aims, as presented in Table 1. A listing of research approaches and models which suggests the separate or combinational application of these theories is also presented.

A critical analysis of ISO17799

ISO17799 (ISO/IEC, 2000) provides a set of recommendations for information security management, by proposing security controls which are system-independent and therefore can be implemented in most systems. Nevertheless, it recommends that a risk analysis survey is conducted prior to selecting the security controls to be implemented. Based on the results of this survey organisations may choose to omit some controls or to introduce new ones. However, most organisations avoid significant derogations from the standard list of controls. These controls fall into 10 categories, including security policy, personnel security, access control, etc.

Under the category ''Personnel Security'' we find controls aiming to protect the IS from insider threats, whether accidental or deliberate, which include:

- *Including security in job responsibilities*. This control suggests fully documenting general and more specific security roles and responsibilities, as laid down by the organisation's security policy.
- *Personnel screening*. Staff verification checks are recommended during job applications or promotions. In addition, managers should observe staffs personal, psychological or financial problems that may have security implications.

Table 1 Criminology theories, concepts, and principles in IS security literature

Criminal theories	Focal concept	Basic principles	Related research within IS security literature
General Deterrence Theory (GDT): Beccaria (1963); Blumstein (1978)	Motive	A person commits a crime if the expected benefit outweighs the cost of sanction.	Straub (1990); Straub and Welke (1998); DoD-ITIPT (2000); Parker (1998)
Social Bond Theory (SBT): Hirschi (1969)		A person commits a crime if the social bonds of attachment, commitment, involvement and belief are weak.	Lee and Lee (2002); Agnew (1995); Hollinger (1986); Lee et al. (2003)
Social Learning Theory (SLT): Sutherland (1924); Akers (1977)		A person commits a crime if (s)he associates with delinquent peers, who transmit delinquent ideas, reinforce delinquency, and function as delinquent role models.	Lee and Lee (2002); Skinner and Fream (1997); Hollinger (1993)
Theory of Planned Behaviour (TPB): Ajzen and Fishbein (1980)		A person's intention towards crime is a key factor in predicting his/her behaviour. Intentions are shaped based on attitude, subjective norms and perceived behavioural control.	Lee and Lee (2002); Leach (2003)
Situational Crime Prevention (SCP): Clarke (1980)	Opportunity	A crime occurs when there is both motive and opportunity. Crime is reduced when no opportunities exist.	Willison (2001, 2004)

- *Confidentiality agreement*. The application of this control entails signing of a non-disclosure agreement, as part of the employees' initial terms and conditions of employment, and conducting reviews when changes occur.
- *Security responsibilities in terms and conditions of employment*. Security responsibilities defined by the organisation and relevant legislation, as well as the consequences of their disregard and the spatial and time conditions of their application should be included in employment terms.
- *Information security and training*. Education and training programmes should be followed by all employees, concerning the security policy and procedures, both before acquiring access to information and during the use of information.

ISO17799 also includes security controls aiming to provide protection against third party access. It suggests controls referring to contractors and temporary employees and recommends controlling their access to systems and facilities, adding non-disclosure clauses to contracts or performing personnel checks on temporary employees. Moreover, segregation of duties for critical tasks and asset accountability is recommended, as well as audit processes and tools. Finally, it suggests physical and logical access controls to limit user privileges and their opportunities for misuse.

In the following section we shall further analyse the standard aiming to reveal the criminology theories that underlie the measures against insider threat it proposes. Thus, we shall be able to examine the efficiency of the theoretical basis of the standard. Consequently, we shall show which other theories may offer incentive for effectively confronting the insider threat.

General Deterrence Theory and ISO17799

ISO17799 acknowledges the importance of insider threat and deals extensively with the protection of the IS from this type of threat. The listing of all controls regarding insider threat, as described in the previous section, shows that they follow the *Security Action Cycle* (Straub and Welke, 1998), as their implementation aims to deter, prevent, detect, and provide remedies for the realisation of insider threat.

The Security Action Cycle is a model that realises the fundamental doctrine of General Deterrence Theory, which suggests that when the possibility of punishment is high and the sanction is severe, potential perpetrators will be deterred from committing delinquent acts. Thus, we reach the conclusion that ISO17799 draws on General Deterrence Theory. As evidence of the GDTs strong influence, we show in the following that the standard applies the Security Action Cycle model comprehensively and covers all four stages of the model, as well as its *deterrence feedback mechanism*.

Deterrence

ISO17799 utilizes the basic mechanisms suggested by GDT, such as policies, guidelines and awareness programmes. It emphasises on organisational security policies that clearly define consequences and sanctions to be applied when employees fail to follow them (Höne and Eloff, 2002). It suggests the use of non-disclosure agreements that define sanctions in order to deter employees and contractors from disclosing organisational information. The standard also proposes specific controls concerning the training of employees, aiming to make them aware of their security responsibilities and the sanctions they may face if they fail to comply. It emphasises on achieving the primary goal of the theory, which is to deter computer abusers, by making them aware of the potential sanctions they face.

Prevention

It includes physical and procedural security controls (e.g. physical and logical access control), to prevent employees from misusing their access privileges. Examples of such controls are: the implementation of a physical security perimeter, the use of some visible form of authentication for authorised personnel, different types of logical access control to business assets, and the procedural control of segregation of duties to minimize the possibility of critical security incidents. It proposes the same preventive mechanisms both for threats originating from outside the organisation (intrusion prevention) and for threats originating from insiders (insider abuse prevention).

Detection

The standard recommends the monitoring of system access and use and includes guidelines concerning the proper use of audit mechanisms. The operation of effective monitoring and auditing mechanisms minimizes the likelihood of abusive activities to remain undetected. The main objective of these mechanisms is to associate each and every action in the system with the individual who is responsible for it; thus enabling the enforcement of sanctions and increasing accountability and, consequently, achieving certainty of sanction — one of the main deterrence mechanisms in GDT.

Remedies

ISO17799 recommends a set of controls for responding to security incidents and system malfunctions, as well as for the implementation of business continuity plans. Not only does it describe reporting mechanisms for the employees in the case of an incident, but it also recommends the use of a formal disciplinary process for employees who have violated security policies and procedures. The standard claims that "such a process can act as a *deterrent* to employees who might otherwise be inclined to disregard security procedures".

Deterrence feedback

The standard implements all four stages of the Security Action Cycle and the feedback mechanism, which is necessary for strengthening deterrence. It clearly suggests a 'learning process', which will exploit the information collected through reporting and monitoring of previous security incidents. The aim of this process is to improve "...controls to limit the frequency, damage and cost of future occurrences" and to use this information in order to improve "...the security policy effectiveness, demonstrated by the nature, number and impact of recorded security incidents". It prescribes periodic reviews of the organisation's security policy, which is one of the main deterrence instruments of the standard. The evaluation of the IS management performance and the existence of feedback suggestions for improvement are identified as one of the standard's critical success factors.

Discussion

Based on the preceding analysis of the security controls against insider threat which ISO17799 proposes, we may conclude that the standard draws on the principles of General Deterrence Theory, the traditional criminology theory that was first proposed in the early 1960s. It implements the full range of controls of the Security Action Cycle, which is the application of GDT in the IS security field, and it uses sanctions as the main deterrence mechanism, emphasising both on their clear statement and on their certainty of application. Nevertheless, there is no indication that the standard recommends the use of *severe* sanctions. The standard leaves the definition of the sanctions' severity to the organisation, depending on its legal and regulatory context, as well as its culture.

We should, however, note that the use of sanctions as a deterrent mechanism has been questioned (Lee and Lee, 2002). People do not always make rational and calculated decisions.

Their actions are often dictated by anger, frustration or despair as it is often the case with employees that have been fired, transferred, denied a raise, or employees who face personal or financial problems (Dhillon and Moores, 2001). Moreover, highly sophisticated and self-confident employees often believe that they can ''outsmart'' the security system and manage to avoid detection (Parker, 1998; Wood, 2000). Sophisticated security controls do not deter these employees who consider these technical obstacles as an extra challenge.

An effective IS security management system should be built upon a broader theoretical basis. We have already presented the major criminology theories that suggest alternative approaches towards the prevention of insider abuse. In the next section, we focus on results of our analysis considering the relationship between modern criminology theories and ISO17799, and we suggest possible ways of application so that they could prove beneficial for a more effective IS security management.

Modern criminology theories and ISO17799

Our analysis of ISO17799 did not find any indication that it has been profoundly influenced by any modern criminology theory, other than GDT. It may suggest the implementation of controls that cover few aspects of one or more of these theories, but it fails to implement their core principles and adopt their underpinning philosophy.

According to the Social Bond Theory, the existence of strong social bonds diminishes the probability of delinquent behaviour. However, the standard does not include measures that could strengthen *attachment* to colleagues or the organisation, *commitment* to business goals or *involvement* in the organisation's procedures and events. The only measure that could be associated with this theory is the development of a security policy and the implementation of an awareness programme, which promote *beliefs* that computer abuse is unacceptable within the organisation. Therefore, we conclude that there is a weak association between ISO17799 and SBT.

The analysis of the standard in relation to the Social Learning Theory produces similar results. The aforementioned controls — security policy development and awareness programme implementation — provide negative *definitions* of abusive behaviour, for an employee to adopt. The standard also suggests a disciplinary process for employees who have violated the security policy and this procedure may deter an employee's delinquent behaviour, thus applying the *differential punishment* factor. However, rewards of non-abusive behaviour are not recommended, therefore the *differential reinforcement* factor is not applied. No other controls were found to affect the factors of *differential association* or *imitation*. It is clear that the standard does not take into consideration the social learning process that can affect an employee for or against computer misuse.

The standard is also very weakly associated with the Theory of Planned Behaviour. It fails to provide any means to considerably affect the *attitude* of an employee towards abusive behaviour. It also fails to communicate management's *subjective norms* of such behaviour or to increase employees' motivation to comply with these norms. It applies only the third factor of the TPB; decreasing the *perceived behavioural control* of an employee, by making computer abuse more difficult by means of access control, surveillance and audit.

Finally, the standard contains measures that *increase the difficulty* (access control), *increase the danger of detection* (surveillance, audit) or *remove possible excuses* (security policy, awareness programmes), which are the three core principles of Situational Crime Prevention. However, we could not suggest that the standard reflects the philosophy of the SCP theory, as it doesn't clearly recognize the role of *opportunities' removal* in preventing insider threat. The application of some SCP principles can be attributed to the fact that the theoretical basis of both SCP and GDT is rooted in the criminological perspective of Classical Theory, as opposed to SBT, SLT and TPB that follow the Sociological Theory (Giddens, 2001). We should also mention that both theories, SCP and GDT, consider insider misuse as a rational act and, in addition to their common background, it is expected that they may lead to some common controls. However, these controls are used in a significantly different manner, as SCP focuses on reducing opportunity and GDT on affecting user motivation.

In Table 2, we summarize the results of our analysis of ISO17799 with regard to the adoption of basic theoretical concepts from criminology theories, as has been described up to this point. Table 2 also suggests the level of relation (low, medium or high) between ISO17799 and each criminology theory we have examined.

Although GDT is widely used in the IS field and provides the theoretical background for most security controls (security policy, security mechanisms and awareness programmes), its practical application and effectiveness is currently in

Table 2 Criminology theories and their relation to ISO17799

Criminology theory	Core concepts	Relevant recommendations within ISO17799	Relation between criminology theory and ISO17799
General Deterrence Theory	Deterrence	Security policy, awareness programmes, confidentiality agreements	High relation
	Prevention	Physical and procedural controls	
	Detection	Access monitoring, auditing	
	Remedies	Response to security incidents, reporting mechanisms, disciplinary process	
	Deterrence feedback	Learning from incidents	
Social Bond Theory	Attachment	N/A	Low relation
	Commitment	N/A	
	Involvement	N/A	
	Belief	Security policy, awareness programmes, confidentiality agreements	
Social Learning Theory	Differential association	N/A	Low relation
	Differential reinforcement/ punishment	Disciplinary process	
	Definitions of behaviour	Security policy, awareness programmes, confidentiality agreements	
	Imitation	N/A	
Theory of Planned Behaviour	Attitude	N/A	Low relation
	Subjective norms	N/A	
	Perceived behavioural control	Physical and procedural controls, monitoring of access, auditing	
Situational Crime Prevention	Difficulty increment	Physical and procedural controls	Medium relation
	Danger increment	Access monitoring, auditing, physical controls	
	Benefit reduction	N/A	
	Excuse removal	Security policy, confidentiality agreements, awareness programmes	

question. In (Lee and Lee, 2002), the authors present the results of their research indicating lack of effectiveness of these measures and comment that this can be attributed to their insufficient application in real situations, but can also be attributed to the fact that the underlying theory fails to cover all aspects of the problem.

Contrary to other theories, GDT does not recommend informal controls. Consequently, ISO17799, drawing on GDT, also lacks recommendations concerning the implementation of informal security controls, as our analysis indicated. The only suggestion of such informal controls can be found at the introductory part of the standard, where (a) management support and commitment, (b) security policy's alignment with business goals and (c) effective communication of security goals to employees, are recognised as critical success factors (ISO/IEC, 2000). However, the standard fails to recommend specific actions and lacks guidance on how to implement such controls. SBT, SLT and TPB, driven by the sociological perspective, hold informal controls to be very important; since their underlying philosophy is that the social environment plays a critical role in the formation of motives and intentions by employees.

As we have already described, Social Bond Theory identifies the four social bonds of *attachment*, *commitment*, *involvement* and *belief*. An organisation should try to create bonds of *attachment* between staff and senior management. The need for management to act as a role model of security behaviour becomes essential. As Leach (2003) suggests, an organisation should ensure that employees feel strongly bounded by their psychological contracts with the company. The only way to achieve such *commitment* to business goals and loyalty to the organisation is by making sure that the company is honoring its part of the contract. The *involvement* bond can be strengthened by encouraging the participation in informal meetings and by allowing the development of social relationships within the organisation; thus promoting a team spirit. Similarly, involvement of employees in all phases of security design and implementation increases their motivation and enforces their *belief* in the fairness of the purposes served by security controls. Practices that promote the above four elements enforce the effectiveness of security controls and policies. On the contrary, security controls that have been imposed on employees in an authoritative manner may be undermined by a feeling of exclusion or detachment provoked on employees.

The Social Learning Theory attributes delinquent behaviour to the association of an individual to delinquent peers. It suggests that, observing other employees' security behaviour can be more influential than attending a security awareness programme or signing a confidentiality agreement. An organisation should be assisted in ways of promoting positive *differential association* and *imitation*. Thus, leadership in the security effort becomes very important, as employees would associate with leaders who serve as models of behaviour and draw admiration and respect. If the security policy is badly formulated in an organisation, then the employee is highly unlikely to follow it, even if it prescribes sanctions for such behaviour (Leach, 2003). For example, if senior management does not follow the security policy and bypasses procedures, then positive *definitions* of computer abuse are conveyed to employees and respect to the security policy is diminished. It is also highly recommended to reward staff for good security behaviour and to provide additional training or to take other appropriate measures for staff who demonstrate unacceptable behaviour (Leach, 2003), in order to apply the *social reinforcement/ punishment* factor.

The Theory of Planned Behaviour focuses on intentions as a key determining factor of social behaviour. Employees' intentions toward IS security are initially influenced by their *attitude* towards computer abuse. It is suggested that personnel screening at the time of employment can provide the organisation with indications about positive or negative attitude towards insider misuse. Attitude can also be influenced through strengthening the employee's bonds to the organisation, as suggested by SBT (Lee and Lee, 2002). Intentions are also formed based on the *subjective norms* that prevail in the organisation. Thus, the development of a social environment that drives employees away from abusive behaviour may prove equally important as the installation of sophisticated security mechanisms. However, in order for an intention to become action, a strong *perceived behavioural control* is needed. Therefore, employees should be given the technical means and the proper training that will allow them to contribute to the protection of the IS.

Situational Crime Prevention suggests that an attempt to face the insider threat focusing solely on employees' motives, without paying attention to the environment in which insider abuse takes place, will also, most likely, prove ineffective. Whereas ISO17799 does include a few security controls that SCP would also recommend (e.g. access control), it is still deprived of its theoretical background and principles. Therefore, an organisation that applies ISO17799 does not make use of the full range of measures suggested by SCP, thus attributing limited significance to the available opportunities an employee has to commit computer abuse, which is a factor recognised as highly important by many researchers (Wood, 2000; Parker, 1998; Dhillon and Moores, 2001). The research on the practical implementation of this theory in the IS field is also in its early stages. However, researchers, such as Willison (2001, 2004), are exploring the application of such controls to information systems, suggesting that an organisation should adopt mechanisms that increase the difficulty and danger of an abusive act, decrease the benefits of such an act and remove possible excuses an offender can use to justify his/her actions.

Implications for research and practice

Having its roots in BS7799, ISO17799 is widely applied in the UK. However, the Information Security Breaches Survey of the UK Department of Trade and Industry for the year 2004 (DTI, 2004) reports that 67% of the organisations are moving towards compliance with the standard observed low or significant change of attitude and behaviour in point of personnel security. Though this number is encouraging, the survey also reveals a significant increase in staff misuse of information systems, especially in large organisations.

Current practice addressing the insider threat entails implementing guidelines proposed by widely accepted security management standards and best practices, such as the ISO17799 standard. However, the increasing occurrence rate of security incidents related with insiders can only be partly explained by the poor or ineffective implementation of such controls. Our analysis indicates that the theoretical background upon which security controls draw, may also provide with an explanation with regard to their ineffectiveness. This is mainly because different theories place importance on different issues, such as the power of deterrence mechanisms, the efficacy of personal beliefs and subjective norms and so on, thus proposing the relevant controls accordingly. Our analysis, though, indicates that to efficiently address the insider threat, all aspects of human behaviour should be taken into consideration, and a holistic approach should be adopted.

The exclusive use of any one of the criminology theories described in this paper cannot be safely recommended, since their effectiveness has not been fully tested within the IS field. Moreover, the tools and techniques implementing their theoretical concepts and recommendations in the context of IS security management are not evident. Most of these theories are constantly gaining support, but IS security management lacks appropriate controls that would implement the principles of these theories and, thus, address the issue of insider abuse in a practical manner.

We argue that any attempt to address the insider threat should be informed by the different views each theory adopts and, accordingly, to implement recommendations from different theories. In our point of view, an important aspect of insider threat is the way an employee forms his/her motivation and intention towards computer abuse. This is probably one of the most difficult aspects of the problem, as it relates to human psychology and social interaction. ISO17799 addresses this issue by proposing a mechanism of sanctions, although severe sanctions have been proven to be rather ineffective in practice. Under our perspective, ISO17799 should follow the suggestions of theories such as SBT, SLT and TPB, by proposing measures that aim to change the norms and ideas concerning security issues.

To holistically address IS abuse within organisations, we propose that models, tools and techniques of IS security should be informed by the core concepts of all criminology theories as they have been described in this paper. In other words, we propose that a multi-methodology approach be employed with regard to insider threat. These criminology theories stem from different scientific paradigms; therefore their combinational application is not straightforward. However, we believe that they are not incommensurable and that their underlying assumptions are reconcilable, in the context of methodological pluralism (Mingers, 1997). Under this perspective our analysis, as well as relevant literature discussed in the beginning of this paper, drives to the conclusion that to study and manage a highly complex as well as critical issue, such as IS insider misuse, a comprehensive and multiparadigm approach is needed. We believe that both research and security management practice can benefit from incorporating basic tenets from criminology theories.

Conclusions

Insider threat is an issue with augmenting importance for IS security management. Tools and methods that are currently applied in the effort to confront this type of threat have their roots in the scientific field of criminology. Analysing ISO17799, the dominant standard in IS security management, we ascertained that it follows the General Deterrence Theory, the most classical and oldest criminology theory. Consequently, it emphasises on measures such as posing sanctions, reinforcing access control, and implementing training and awareness programmes.

Nevertheless, the adoption of a single theory and especially a theory that has been heavily criticized by social researchers impoverishes the arsenal of IS security management. We have argued that IS security management would benefit from enrichment with ideas from other well-established criminology theories and the relevant standards should encourage this pluralistic approach.

Moreover, we believe that the IS security field would also benefit from an intellectual engagement with other disciplines studying the nature of human behaviour, such as sociology and criminology. This interaction, that should be further explored, would provide IS security researchers, as well as practitioners, with more insight as to the nature of computer abuse and possible ways to handle with it.

Acknowledgements

We would like to record our thanks to the anonymous referees and the editor of this journal for their constructive criticism, which led to a substantial improvement of the style of the paper.

References

Agnew R. Testing the leading crime theories: an alternative strategy focusing on motivational process. Journal of Research in Crime and Delinquency 1995;32(4):363—98.

Ajzen I, Fishbein M. Understanding attitudes and predicting social behaviour. Englewood Cliffs, NJ: Prentice-Hall; 1980.

Ajzen I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behaviour. Journal of Applied Social Psychology 2002;32:665—83.

Akers RL. Deviant behavior: a social learning perspective. Belmont, CA; 1977.

Beccaria C. On crime and punishments. Indianapolis, IN: Bobbs Merril; 1963.

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

Clarke RV. Situational crime prevention: theory and practice. British Journal of Criminology 1980;20:136—7.

Department of Defense, Insider Threat Integrated Process Team (DoD-ITIPT). DoD insider threat mitigation. U.S. Department of Defense; 2000. Available online at http://www.defenselink.mil/c3i/org/sio/iptreport4_26dbl.doc [accessed 01-Apr-05].

Department of Trade and Industry. Information security breaches 2004. Available online at http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf; 2004 [accessed 01-Apr-05].

Dhillon G, Moores S. Computer crimes: theorizing about the enemy within. Computers and Security 2001;20(8):715—23.

Giddens A. Sociology. 4th ed. Cambridge, UK: Polity Press; 2001.

Hinde S. The law, cybercrime, risk assessment and cyber protection. Computers and Security 2003;22(2):90—5.

Hirschi T. Causes of delinquency. Berkeley, CA: University of California Press; 1969.

Hollinger RC. Acts against the workplace: social bonding and employee deviance. Deviant Behaviour 1986;7:53—75.

Hollinger RC. Crime by computer: correlates of software piracy and unauthorized account access. Security Journal 1993; 4(1):2—12.

Höne K, Eloff JH. Information security policy — what do international information security standards say? Computers and Security 2002;21(5):402—9.

ISO/IEC. Information technology — code of practice for information security management. ISO/IEC 17799: 2000(E), Geneva, Switzerland; 2000.

Leach J. Improving user security behaviour. Computers and Security 2003;22(8):685—92.

Lee J, Lee Y. A holistic model of computer abuse within organisations. Information Management and Computer Security 2002;10(2):57—63.

Lee SM, Lee S, Sangjin Y. An integrative model of computer abuse based on social control and general deterrence theories. Information and Management 2003;41(6):707—18.

Magklaras GB, Furnell SM. A preliminary model of end user sophistication for insider threat prediction in IT systems, Computers and Security, in press. doi:10.1016/j.cose.2004.10.003.

Mingers J. Multi-paradigm multimethodology. In: Mingers J, Gill A, editors. Multimethodology: the theory and practice of combining management science methodologies. J.Wiley & Sons Ltd; 1997. p. 1—20.

Neumann PG. The challenges of insider misuse. In: Proceedings of the workshop on preventing, detecting, and responding to malicious insider misuse. Santa Monica, CA: RAND Corp; August 1999.

NSTISSAM. Advisory memorandum on the insider threat to U.S. government information systems. US NSTISSC. Available online at http://www.cnss.gov/; 1999 [accessed 01-Apr-05].

Parker DB. Fighting computer crime: a new framework for protecting information. New York, NY: John Wiley and Sons; 1998.

Porter D. Insider fraud: spotting the wolf in sheep's clothing. Computer Fraud and Security 2003;2003(4):12—5.

Schultz EE. A framework for understanding and predicting insider attacks. Computers and Security 2002;21(6):526—31.

Skinner WF, Fream AM. A social learning theory analysis of computer abuse among college students. Journal of Research in Crime and Delinquency 1997;34(4):495—518.

Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviours. Computers and Security 2005;24(2):124—33.

Straub DW. Effective IS security: an empirical study. Information System Research 1990;1(3):255—76.

Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS Quarterly 1998;22(4):441—65.

Sutherland E. Criminology. Philadelphia: J.B. Lippincott; 1924.

Tuglular T. A preliminary structural approach to insider computer misuse incidents. In: Proceedings of EICAR 2000 international conference, Brussels, Belgium; March 2000.

Vardi Y, Wiener Y. Misbehavior in organisations: a motivational framework. Organization Science 1996;7(2):151—65.

Willison R. Understanding and addressing criminal opportunity: the application of situational crime prevention to IS security. Working Paper Series 100. Department of Information Systems, London School of Economics and Political Science; 2001.

Willison R. Understanding the offender/environment dynamic for computer crimes: assessing the feasibility of applying criminological theory to the IS security context. In: Proceedings of the 37th Hawaii international conference on system sciences; 2004.

Wood BJ. An insider threat model for adversary simulation. In: Anderson R, Bozek T, Longstaff T, Meitzler W, Skroch M, van Wyk K, editors. Research on mitigating the insider threat to information systems — #2. Santa Monica, CA: RAND Publ.; 2000.

Marianthi Theoharidou is currently commencing her Ph.D. research in Athens University of Economics and Business (AUEB) at the Department of Informatics. She holds a B.Sc. in Informatics and an M.Sc. in Information Systems, both acquired from Athens University of Economics and Business. Her research interests include information systems security management, risk assessment and management and healthcare information systems.

Spyros Kokolakis is a Lecturer at the Department of Information and Communication Systems Engineering at the University of the Aegean, Greece. He received a B.Sc. in Informatics from the Athens University of Economics and Business in 1991 and a Ph.D. in Information Systems from the same university in 2000. His current research interests include information systems security management, risk analysis, and security policies design and implementation. He is a member of IEEE and ACM.

Maria Karyda holds a Ph.D. in Information Systems from the Department of Informatics, Athens University of Economics and Business, Greece. She obtained a B.Sc. in Informatics and an M.Sc. in Information Systems from the same university in 1998 and 2000, respectively. Her research interests include organisational aspects of information systems security management, the use and application of security policies and security culture and awareness.

Evangelos Kiountouzis is a Professor of Information Systems at the Department of Informatics of the Athens University of Economics and Business, Greece. He studied Mathematics at the University of Athens, Greece, and received a Ph.D. in Informatics from the University of Ulster, UK. His professional and research interests focus on information systems analysis and design methodologies and on information systems security management. He is the author of several books on the topics of information systems and information systems security management and he has published numerous papers in international conferences and journals.