Motivations for Employee Computer Crime

Understanding and Addressing Workplace Disgruntlement through the Application of Organisational Justice

Willison, Robert

Motivations for Employee Computer Crime: Understanding and Addressing Workplace Disgruntlement through the Application of Organisational Justice

Robert Willison

Department of Informatics

Copenhagen Business School

rw.inf@cbs.dk

Working Paper nr. 1, 2009

ISBN: 978-87-89550-40-4

Abstract

Within the IS security field, employee computer crime has received increased attention. Indeed, a number of researchers have focused their attention on the behaviour of the 'insider', both prior to and during the perpetration. Despite this, there is currently an absence of academic insight into the problem of workplace disgruntlement and how this may motivate employee computer crime. To address this deficiency, this paper draws on a body of knowledge called 'organisational justice', which examines how perceptions of fairness are formed. Under this umbrella term are four constructs which relate to different organisational phenomena and influence employees' fairness perceptions. It is believed that these constructs, entitled distributive, procedural, interactional and informational justice, and the theories which underpin them, can not only assist in understanding, but also in mitigating disgruntlement. To illustrate this, a case of employee computer sabotage is analysed, highlighting which forms of organisational justice occurred, and how they could have been addressed. The discussion section notes how mitigating disgruntlement provides a new area for safeguard implementation, with the final part of the paper discussing the conclusions and potential for future research.

Introduction

IS security practitioners are responsible for addressing a wide range of threats, not least that of the 'insider'. While attempts to gain accurate statistics on employee computer crime are seriously hamstrung by organisational under-reporting, based on fears of reputation damage, security surveys at least provide some indication of the problem. The UK National High Tech Crime Unit (2005) reported that 38% of financial fraud, 68% theft of information/data, and 100% sabotage to data or networks were committed internally. These figures are supported by the 2006 Deloitte Global Security Survey which reported that, of those organisations which experienced breaches, just under half were committed inside the company. Two more recent surveys have provided equally worrying data. The Pricewaterhouse Coopers/UK Department for Business Enterprise and Regulatory Reform survey (PwC/DoBERR, 2008) notes how for large organisations (250+ employees) 57% of respondents reported that the cause of the their worst security incident to be internal, while the Global State of Information Security survey (PwC/CSO/CIO, 2008) showed that employees (former and current) formed the biggest threat for respondents.

Given the above, researchers have turned their attention to the insider threat. More specifically, a number have focussed on areas related to offender behaviour, both prior to and during the perpetration of employee computer crime. Currently, however, there has been a lack of academic insight into the problem of employee disgruntlement and how this plays a role in motivating some form of insider computer crime. A report by the US Secret Service and Carnegie Mellon (USSS/Carnegie Mellon, 2005), studied 49 cases of insider sabotage. One of the key findings notes how in 88% of the cases, the perpetrator held a 'work-related grievance' before the act of abuse. This is accompanied by another key finding which views these grievances as a 'trigger' for their criminal actions.

The report (USSS and CERT, p. 3) notes for example, how:

> A city government employee, who was passed over for promotion to finance director retaliated by deleting files from his and a co-worker's computers the day before the new finance director took office. An investigation identified the disgruntled employee as the perpetrator of the incident.

This paper, therefore, focuses on the issue of workplace disgruntlement. To address this problem, and the associated deficiency in the current literature, an existing body of research, which examines the issue of fairness, is utilised. This body of research falls under the umbrella term 'organisational justice'. There are four main constructs which relate to different organisational phenomena, and influence employees' perceptions of fairness. It is believed that these constructs (entitled distributive, procedural, interactional and informational), and the theories which underpin them, can not only assist in understanding, but also in mitigating disgruntlement.

A better understanding of how disgruntlement is created provides the ability for it to be addressed, and therefore enhances security efforts by expanding the range of control for companies. New safeguards can therefore be introduced to address this 'trigger', for while corporations may rely heavily on controls to deter or prevent employee computer crime, why not mitigate disgruntlement and thereby forestall criminal behaviour in the first instance?

The next section of the paper reviews the literature related to employee computer crime, and highlights the related deficiencies. This is followed by a description of the constructs advanced in this paper, namely Distributive, Procedural, Interpersonal and Informational justice. How organisational justice can be applied to IS security forms the next section, with the discussion and conclusion forming the penultimate and final sections, respectively.

Literature review

This section of the paper reviews the related literature, which divides into three areas including offender deterrence, the intention of potential offenders, and the prevention of employee computer crime.

Deterrence

The issue of deterring employee computer crime has been addressed by several IS security researchers (Campbell, 1988; Cardinali, 1995; Harrington, 1996; Hoffer and Straub, 1989; Sherizen, 1995; Straub, 1990; Straub and Nance, 1990; Straub and Welke, 1998). More specifically, a number have employed General Deterrence Theory (GDT) for studying this phenomenon (Harrington, 1996; Hoffer and Straub, 1989; Straub, 1990; Straub, Carlson and Jones, 1992; Straub and Welke, 1998). Central to this theory is the role played by sanctions (Cook, 1982), in terms of their perceived certainty and severity by the offender. Hence, the theory postulates that if an offender perceives the certainty and severity of sanctions, associated with a crime, as high, then this will deter them from engaging in the criminal act (Straub, 1990).

Straub (1990) applies GDT to examine whether organisational expenditure on IS security results in improved security. Based on a survey of 1,211 organisations the results reported that expenditure on deterrent procedures and prevention safeguards will reduce the incidents of computer abuse. In a later paper, Straub and Welke (1998) examine the extent to which managers are aware of the range of actions available to them when addressing systems risk. As part of the research, a 'security action cycle', based on GDT, is advanced. This framework consists of four separate, but related activities, which include i) deterrence, ii) prevention, iii) detection and iv) recovery. These four areas are designed to enhance IS security by reducing systems risk. Hence, the initial aim of the IS security countermeasures strategy would be to deter such

activity. If deterrence proved ineffective, the second part of the strategy would aim at preventing the offender from perpetrating computer crime, and so on. Straub and Welke (1998) argue that with regard to GDT, the four elements of the security action cycle can all contribute to the deterrent effect i.e. when systems security is taken seriously by an organisation, the potential offender will perceive the certainty and severity of sanctions as high, and they will be deterred.

Intention

In a bid to achieve a more detailed understanding of offender behaviour prior to the act of perpetration, some researchers have combined GDT with other theories to understand the intention of potential offenders (Lee and Lee, 2002; Lee et al, 2004; Workman and Gathegi, 2007). Lee and Lee (2002) advance a 'holistic' model of employee computer crime based on GDT, Social Bond Theory (SBT), and Social Learning Theory (SLT). They draw on the Theory of Planned Behaviour (TPB) to provide an over-arching framework, with its focus on intention. Lee and Lee (2002) therefore relate SBT, SLT and GDT to the three factors as advanced by TPB which constitute intention i.e. 'attitude', 'social norms' and 'perceived behavioural control'. As the name suggests, Social Bond theory asserts that there are four factors (attachment, commitment, involvement and beliefs) which constitute a social bond between an individual and society. The weaker the bonds, the more likely an individual will undertake criminal behaviour. Given this, Lee and Lee (2002), equate the four factors as influencing an individual's 'attitude'. In addition, the authors equate 'social norms' with Social Learning Theory. The latter asserts that an individual is more likely to engage in crime if they associate with others who themselves commit crime, transmit deviant values and function as criminal role models. Finally, Lee and Lee (2002) note how deterrence (as defined by GDT) will influence an individual's 'perceived behavioural control'. Hence, the three theories incorporated within Lee and Lee's (2002) model incorporate factors which they believe influence 'attitude', 'social norms' and 'perceived behavioural control', which further influence the 'intention' to commit employee computer crime.

Similarly, Lee et al (2004) also use the Theory of Planned Behaviour for an over-arching framework, and draw on General Deterrence Theory and Social Control Theory (which is a forerunner to Social Bond Theory). Unlike Lee and Lee (2002), Lee et al (2004) focus on two factors which influence the 'intention' to undertake computer crime. Therefore, 'security policy', 'security awareness' and 'security system' are thought to impact on 'intention' by acting as deterrent factors. In addition, the four factors addressed by Social Control Theory, which create a social bond (as previously advanced by Social Bond Theory) are equated by Lee et al as 'organizational trust'. Hence, the social bond (level of trust) between an individual and the organisation in which they work will influence the 'intention' to commit computer abuse.

Prevention

As noted above, companies can consider safeguards in terms of four categories which include deterrence, prevention, detection and remedies (Straub and Welke, 1998). Despite this, Willison (2006) notes how with regard to the existing literature on employee computer crime, there is currently a lack of insight into the relationship between the offender and the context during the perpetration of employee computer crime. Admittedly, Straub and Welke (1998) discuss preventive controls (designed to stop perpetration), but from a theoretical perspective, only in terms of their deterrent effect. Once the offender moves beyond the point of deterrence and embarks on a criminal act GDT is limited. GDT is therefore, unable to provide any theoretical insights into the actual act of perpetration. As noted, Lee and Lee (2002), and Lee et al (2003) draw on the over-arching framework of the Theory of Planned Behaviour, which focuses on the offender's intention to commit such abuse. However, while it has been noted that intention is a major factor in determining whether an individual undertakes a specific form of behaviour, this does not provide any insight into the actual criminal act.

An alternative perspective is therefore provided by recent work which draws on crime prevention theories (Willison, 2006a; Willison and Backhouse, 2006). More specifically, in a bid to throw light on the offender/context dynamic, Willison (2006) advances two criminological approaches entitled the Rational Choice Perspective and Situational Crime Prevention. Unlike dispositional criminological theories, which focus on the causes of criminality, Situational Crime Prevention and the Rational Choice Perspective afford consideration of the criminal act. Willison (2006) argues that the Rational Choice Perspective and Situational Crime Prevention offer a theoretical basis on which to analyse the offender/context relationship by examining the stages an offender must go through in order for a crime to be committed.

Deficiencies of the existing literature

Despite these insights provided by the existing literature into employee computer crime, there is currently an absence of research into employee disgruntlement and how this may motivate an individual to perform these crimes. Admittedly, external factors (e.g. marital breakdown, financial problems and addictions in their various guises) can play their role (Essinger, 1990; Comer; 1998: Willison, 2002), but this paper focuses on the organisational context. Of great importance is the recognition that as factors within the organisational context creates disgruntlement, there at least exists the potential for addressing the problem. In a bid to achieve this aim, this paper draws on a body of literature which examines employee perceptions of fairness/unfairness in organisations, or what is interchangeably termed justice/injustice. More specifically, this paper addresses those factors which may lead an employee to perceive that they have been treated unfairly. Four fairness constructs are therefore discussed, which collectively fall under the umbrella term organisational justice. It is argued that perceived injustice by an employee leads to disgruntlement, which may help to motivate the individual to undertake some form of computer crime.

Organisational justice

Before the organisational justice constructs are discussed, it is important to note two points. First, as the number of studies has increased, so too have the theoretical approaches used to study constructs (Colquitt et al 2001). Hence, there are a plethora of theories used to underpin research in this area. Given space limitations, the plurality of theories and the related voluminous body of literature, specific reference will only be made to the constructs. Second, just as there is a lack of consensus over appropriate theory, so too is there disagreement over the main constructs. Some researchers, for example, perceive there to be three, while others perceive four (Colquit, 2001). This paper discusses four constructs (Colquitt, 2001), which are now described.

Distributive justice

Organisational justice has been researched by social psychologists for over forty years (Nowakowski and Conlon, 2005). More specifically, Greenberg (1990a) describes this body of literature as 'grown around attempts to describe and explain the role of fairness as a consideration in the workplace' (p. 400). Initial research focused on the fairness (justice) of decision outcomes in the organisational context, termed distributive justice (Nowakowksi and Conlon, 2005). The latter is perceived to occur when the outcomes are considered to be consistent with implicit rules (norms) for allocation, such as equity (Adams, 1965; Deutsch, 1975; Leventhall, 1976). Indeed, Leventhal (1976) defined the equity rule as 'a single normative rule which dictates that rewards and resources be distributed in accordance with recipients' contributions' (p.94). When employees perceive a 'breach' of these rules, then perceptions of injustice ensue. Hence, employees might perceive various outcomes (e.g. no pay rise, no promotion) as unjust, when relative to their contributions in terms of, for example, the quantity and quality of their work (Walster et al, 1978). Equity is not the only implicit norm which might be applied to assess a fair outcome. Other allocation rules include equality and need.

Procedural Justice

Development in the justice literature occurred with research on procedures. Unlike its distributive counterpart, original work in this area related not to the organisational, but rather the legal context (Colquitt et al, 2001). Researchers in the fields of psychology and law noted how participants in dispute resolution (e.g. arbitration and mediation) cases reacted to not only the outcomes (i.e. the focus of distributive justice), but also to the procedures used to determine the outcomes. There subsequently emerged the construct of procedural justice, defined as the perceived fairness of the procedures used to determine outcomes. Thibaut and Walker's (1975) seminal work in this area notes not only the importance of the distribution (i.e. the outcome of arbitration and mediation) but also the degree of influence individuals have during the process. Specifically, Thibaut and Walker, (1975) examine the 'process control' of individuals in dispute resolution cases. This 'control' refers to the degree to which individuals are able to voice their opinions, during the process, and the amount of time given to do so. Hence, their research indicates that perceptions of fairness occur if individuals feel they have the opportunity to voice their opinions in an adequate period of time.

While Thibaut and Walker's (1975) work focussed on the legal context, it was the research of Leventhal and his colleagues (Leventhal, 1980; Leventhal et al, 1980), who first studied procedural justice in the organisational context. Departing from a focus on process control, Leventhal focuses on the nature of the procedures and the implications for procedural justice perceptions. Six rules are identified, which, if followed, would lead to the development of fair procedures. As Cohen-Charash and Spector (2001, p.280) note, these rules include:

> a) the consistency rule, stating that allocation procedures should be consistent across persons and over time; b) the bias suppression rule, stating that personal self-interests of decision-makers should be prevented from operating during the allocation process; c) the accuracy rule, referring to the goodness of the information

> used in the allocation process; d) the correctability rule, dealing with the existence of opportunities to change an unfair decision; e) the representativeness rule, stating that the needs, values, and outlooks of all the parties affected by the allocation process should be represented in the process; and f) the ethicality rule, according to which the allocation process must be compatible with fundamental moral and ethical values of the perceiver.

Interpersonal and Informational Justice

Yet further development in the justice literature occurred as a result of insights garnered from procedural research. It was noted how, for example, even within an organisation, if a policy was considered fair, employee perceptions of injustice could result. Given this, and other observations, 'interactional justice' was first proposed by Bies and Moag (1986), whereby this form of justice is fostered when those in authority show respect and sensitivity to employees, while explaining the rationale for their decisions. Bies and Moag's (1986) research into employee recruitment, therefore, considers interactional justice to comprise four elements which include truthfulness (e.g. candidness and the absence of deception), respect (e.g. politeness as opposed to rudeness), propriety of questions (e.g. the absence of prejudicial statements or improper remarks), and justification (e.g. with regard to explaining a decision).

Later work by Greenberg (1990b, 1993) split interactional justice into two other constructs entitled 'interpersonal' and 'informational'. Greenberg (1990b, 1993) views aspects of interactional justice ('respect' and 'propriety') to be more appropriately conceptualised as interpersonal justice, and closely related to its distributive counterpart. Hence, even if an outcome leads to perceptions of distributive injustice by an employee, perceptions of interpersonal justice may moderate this feeling, leaving the employee feeling better about the situation. Greenberg (1990b, 1993) further asserts that elements of interactional justice, which focus on how decisions are explained ('truthfulness' and 'justification') may best be viewed as 'informational' justice. In addition, Greenberg notes how this form of justice is closely related to its procedural

form. Hence, information provided by those in authority, and during the course of an explanation of a particular decision, may enable staff members to more accurately assess procedures. Later research by Shapiro et al. (1994) highlights additional informational justice factors with regard to explanations by those in positions of authority. Hence, perceptions of informational justice are enhanced when explanations are considered by employees to be timely, reasonable and specific, with regard to the recipients' needs.

For the purposes of this paper, it is important to consider the 'outcomes' which impact organisations, and occur as a consequence of perceptions of justice/injustice. Indeed, this area has been addressed by a considerable body of research. Conducting a meta-analytic review, based on 183 studies, Colquitt et al (2001) identify eleven broad categories of outcomes which include 'outcome satisfaction', 'performance' 'organisational citizenship behavior: individual-referenced', 'organisational citizenship behavior: system-referenced', 'withdrawal', 'negative reactions', 'evaluation of authority: agent-referenced', evaluation of authority: system referenced', 'trust', 'job satisfaction' and 'organisational commitment'. It is worth noting that within the category 'negative reactions' are placed organisational justice studies which have found an empirical link between perceptions of injustice and theft (Greenberg, 1990, 1993), retaliation (Skarlicki and Folger, 1997; Skarlicki et al, 1999), revenge (Bies and Tripp, 1996), workplace violence (Greenberg and Barling, 1999) and sabotage (Ambrose et al, 2002; Skarlicki and Folger, 1997; Giacolone et al; 1997).

The application of organisational justice to the IS security domain

Considering disgruntlement in terms of organisational justice affords an understanding into the dynamics of this problem. Clarity with regard to the constructs is of key importance as this enables specific identification of the organisational phenomena, which create the different forms of injustice, and by so doing aids their mitigation. This

section of the paper advances an example of disgruntlement and discusses the forms of injustice which ensued, and how they could have been addressed. The case in question involved a female database expert (USSS/CERT, 2005, p. 37)

> After more than four years of successful service marked by stellar performance reviews, management commendations, and nomination for the organization's executive training program, a female employee filed multiple complaints with human resources against her male supervisor and male co-workers. She claimed her co-workers had made sexual remarks, overridden her technical decisions regarding databases (an area in which she was considered an expert), and contacted her team's contractors regarding her projects without her knowledge. No action was taken by human resources, and the actions by her co-workers continued. The employee's performance reviews declined sharply in the next two years, and she was demoted. Subsequent complaints to her supervisor resulted in a suspension for insubordination. Almost a year following her written complaint to human resources, she resigned and began employment with another organization. Two months later, she learned that only her more recent, negative performance reviews were forwarded to her new employer. She used one of several shared DBA accounts to delete critical table spaces in the [former] organization's Oracle database, deleting crucial data. Due to a coincidental problem with database backups during the same time period, 115 employees had to spend 1800 hours to recover and re-enter lost data.

This example can be analysed and explained by drawing on the different forms of organisational justice. Initially the female database expert filed multiple complaints to the HR department with regard to her male supervisor and male co-workers. These complaints related to sexual remarks, overriding her database technical decisions, and the contacting of her team's contractors without her knowledge. Despite the complaints, the HR department failed to act and the employee's supervisor and co-workers continued with their behaviour. The fact that no action was taken by the HR department can be viewed as leading to procedural injustice. As noted, Leventhal (1980) highlights six rules which, if followed, lead to the development of fair procedures.

Assuming the organisation had HR procedures in place, then clearly at least two of these rules, entitled the 'consistency' and 'representativeness' rules, were absent. The former concerns the need for procedures to be applied consistently across staff and over time. The latter requires outlooks, values and needs to be represented in a procedure. If these two rules had been applied to the case in question, then the ensuing disgruntlement in the form of procedural injustice could possibly have been forestalled.

At another level, it can be argued that the female database expert had no 'process control' (Thibaut and Walker, 1975), which also led to perceptions of procedural injustice. In other words, she had no opportunity to 'voice' her concerns to the relevant parties. Although complaints were filed by the employee, these fell on deaf ears, leaving the employee with no chance to discuss her grievances. This lack of process control relates to the consistency and representativeness rules discussed above. If the HR procedures had been applied (consistency rule) and if the concerns of the female database expert had been acted upon and considered (representativeness rule), then it is more than likely that she would have been given the appropriate opportunity and time (i.e. process control) to discuss her complaints. As the organisation failed to act, the HR department missed their opportunity to counter procedural justice. In addition, the consequential absence of process control probably enhanced the employee's feeling of disgruntlement.

After the failure by the HR department to act on her complaints, the employee's productivity suffered leading to poor performance reviews. Interestingly, one 'outcome' which can occur as a result of perceptions of injustice is that of declining 'work performance' (Cohen-Charash and Spector, 2001). In fact, the employee's performance suffered to such an extent that she was subsequently demoted. There is the possibility here that the employee might have perceived distributive injustice. Despite the poor performance reviews, the employee might have considered a demotion unfair in light of her highly successful previous four years, where she received outstanding performance

appraisals. Although not discussed in the case, informational injustice might also have occurred if the decision to demote the employee was not clearly explained and discussed with her.

After further complaints, the employee was suspended for insubordination. Following these struggles, the employee left to work for a new company. Two months into her new job, she learned her previous organisation had only passed on to her new employer, work performance reviews covering the period when her productivity had been in decline. Hence, the reviews covering the period when she was considered a 'stellar' performer were omitted. In this instance, the employee probably experienced further procedural injustice. If the employee was offered a new job based on a probationary period, a decision to employ her after that period might have included performance reviews from her previous employer. If this were the case, then she probably perceived procedural injustice, as not all the relevant information (i.e. the good performance reviews) were not sent to her new company, to enable a fair decision to be made. In connection with this point, Leventhal (1980) highlights, as one of the six rules for enabling fair procedures to be created, the role of accurate information. Hence, the accuracy rule notes the need for sound information to be used in the process. If her previous employer had sent on all her performance reviews then perceptions of procedural justice would probably not have occurred.

These final actions by her former company led the employee to remotely access their Oracle database using a still active shared DBA account. She then went on to delete critical table spaces with the consequence of destroying important data. As noted, organisational justice studies have found an empirical link between perceptions of injustice and sabotage (Ambrose et al, 2002; Skarlicki and Folger, 1997; Giacolone et al; 1997). This is further supported by the US Secret Service and Carnegie Mellon report, which highlights the link between disgruntlement and sabotage (USSS/CERT 2005).

The analysed example indicates how organisational justice can explain the causes of disgruntlement. In addition, by so doing, this body of knowledge can further provide explicit guidance in forestalling the problem in the first place. As Nowakowski and Conlon (2005, p. 7) state:

> A key advantage … is that by distinguishing specific forms of justice, one can more easily identify elements of procedures that might be lacking in some areas, and thus recommend changes to the procedures themselves or the behaviour of those involved in order to enhance perceptions.

Understanding the specific forms of organisational justice also affords the potential to optimise an organisation's safeguard options, and thereby dissipate even pre-existing disgruntlement. An employee, for example, may perceive distributive injustice as a result of not receiving an expected pay rise. However, this feeling of disgruntlement may be tempered via informational justice. Therefore, if a manager provides an explanation, about why no pay rise was given, which is perceived by the employee to be thorough, timely, reasonable, specific, and honest, then the initial feeling of disgruntlement may decrease. Attempts to address existing disgruntlement may also be enhanced through interpersonal justice. The same manager, while providing the explanation, will also be 'assessed' by the employee in terms of their politeness, dignity, respect and propriety. If the employee perceives these to be present, then interpersonal justice will impact disgruntlement. Therefore, even if perceptions of injustice are created owing to particular organisational phenomena, they may be tempered through others. This, however, will only be afforded if the particular forms of organisational justice, and the inter-relationships between them, are acknowledged and acted upon.

Of course, organisational justice must be viewed as a double-edged sword. Though interactional and informational justice represent means through which to address disgruntlement, they also offer means through which it can be reinforced. An already

disgruntled employee who receives an unsatisfactory and late explanation, provided by a rude manager, will only experience greater feelings of injustice.

Discussion

Mitigating disgruntlement would be of obvious interest to practitioners, particularly as the organisational justice literature offers the potential to develop a new range of safeguards. Traditionally, countermeasures have been divided into four areas which include deterrence, prevention, detection and recovery (Forcht, 1994; Parker, 1981; Straub and Welke; 1998). Rather ironically, despite the obvious fact that it is people who commit employee computer crime, there is still very little insight into the behaviour of offenders, both prior to and during the commission process (Willison and Siponen, forthcoming). Leaving deterrence aside, prevention measures represent a final opportunity in that this form of safeguard is designed to stop the actual commission. If this group of measures fail, then organisations are in the unenviable position of utilising detection and recovery countermeasures. Admittedly, progress in understanding offender behaviour has been made, but this is through the application of, for example, General Deterrence theory (Straub, 1990; Straub and Welke, 1998) and crime prevention approaches (Willison, 2006, Willison, 2006a), which place the offender centre stage, and so enable their examination. Such is the case with the application of organisational justice. Figure 1 (based on Straub and Welke, 1998) includes the four traditional areas of safeguard application in the form of deterrence, prevention, detection and remedies. These areas each contribute to the deterrent effect, via the 'deterrent feedback' loop. The obvious goal for organisations is to maximise the deterrence and prevention of computer abuse and minimise undetected and unpunished abuse. However, as Figure 1 illustrates, this security action cycle can be extended by addressing the problem of disgruntlement which precedes deterrence. In this sense, practitioners are provided with an additional safeguard application area.

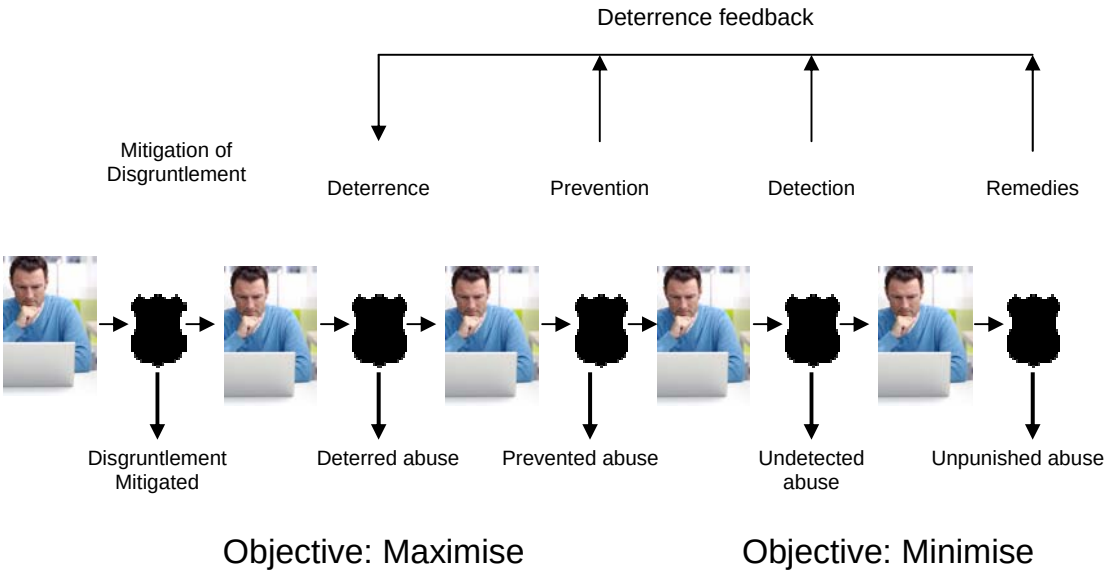

Figure 1: The Extended Security Action Cycle based on Straub and Welke (1998)

To assist in the development of this additional application area, future research could encompass the application of organisational justice through the action research method (Baskerville and Wood-Harper, 1998; Mathiassen, 2002).

Rapoport (1970, p.499) notes how:

> Action research aims to contribute to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework.

In addition to the above, Susman and Evered (1978, p. 588) note how action research aims to develop the self-help competencies of people facing problems'. In this sense the problem would be disgruntlement, and 'self-help competencies' would be developed through intervention in an organisation. This intervention is central as a fundamental contention of action research is that complicated organisational processes can clearly be understood via changes to these processes and studying the effects. Disgruntlement could therefore be researched through the application and delivery of

policies and procedures based on organisational justice. The aim of the research would be to assess the extent to which disgruntlement could be managed in an organisational context.

Conclusion and future research

In the field of IS security there is an increasing body of literature which focuses on employee computer crime. Despite this, the issue of workplace disgruntlement has been overlooked. More specifically, understanding this problem and how it plays a role in motivating some form of insider computer abuse has been neglected by the IS security field. To address this deficiency, this paper draws on a body of research which examines the issue of fairness, entitled organisational justice. There exist four main constructs which relate to different organisational phenomena and influence employees' perceptions of fairness. It is argued these constructs (called distributive, procedural, interactional and informational justice), and the theories which underpin them, can not only assist in understanding, but also in mitigating disgruntlement.

Aside from addressing disgruntlement, organisational justice impacts other areas of IS security. Although relatively unexplored itself, organisational citizenship behaviour (OCB) has become a recent focus for IS security research (Stanton et al, 2004). OCB can be defined as 'behaviors that are discretionary and not explicitly rewarded but can help improve organizational functioning' (Colquitt et al, 2001, p.430). Hence, IS Security research in this area has focussed on the link between OCB and end-users security behaviour i.e. if OCB is withdrawn, what are the implications for this form of behaviour? Importantly, studies in the organisational justice literature have examined OCB with regard to perceptions of injustice. More specifically, several studies have examined the extent to which OCB is withdrawn as a consequence of perceptions of injustice (Eskew, 1993; Tepper and Taylor, 2003). One obvious research area that could be pursued is the extent to which OCB, in the form of compliance to IS security policies or other areas of

end-user security behaviour, is withdrawn by end-users owing to perceptions of injustice.

The organisational justice literature also opens up potential avenues of research with specific regard to IS security policies. While a number of papers have researched the factors which may affect compliance to these policies, there is little research which has focussed on their form (Siponen and Iivari, 2006). One area of future research could therefore consider the relationship between procedural justice and policies. As noted earlier, Leventhal and his colleagues (Leventhal, 1980; Leventhal et al, 1980) focus on the nature of procedures and the implications for procedural justice perceptions. They advance six rules which, they argue, if followed will lead to the development of fair policies. Potential research could therefore consider the design of security based on these policies and the extent to which end users consider the policies as fair and workable.

In conjunction with the above another potential area to consider with regard to IS security policies, is the extent to which end-users have a degree of 'process control' over their design. Thibaut and Walker's (1975) seminal research consider process control in terms of the degree to which individuals are able to voice their opinions during a process, and the amount of time given to do so. Perceptions of procedural justice are expected to occur if individuals are handed the opportunity and time to voice their opinions. If this is the case, potential research could consider end-users and their process control over the design of policies, for as Adams and Sasse (1999, p.45) note:

> Insecure work practices and low security motivation among users can be caused by security mechanisms and policies that take no account of users' work practices, organizational strategies, and usability. These factors are pivotal in the design and implementation of most computer systems today. Designers of security mechanisms must realize that they are the key to successful security systems. Unless security departments understand how the mechanisms they design are used in practice,

> there will remain the danger that mechanisms that look secure on paper will fail in practice.

The organisational justice body of knowledge, therefore, appears to represent a valuable resource for IS researchers. While this paper has focussed on its application for addressing disgruntlement, it is clear that the issue of fairness has the potential for opening up other areas of research.

References

Adams, A. and Sasse, M. (1999) Users Are Not The Enemy. *Communications of the ACM* 42 (12): 41-46.

Adams, J. (1965) Inequity in Social Exchange. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology* (Vol. 2, pp. 267-299). New York: Academic Press.

Ambrose, M., Seabright, M. and Schminke, M. (2002) Sabotage in the Workplace: The Role of Organizational Justice, *Organizational Behavior and Human Decision Processes*, 89, 947-965.

Baskerville, R., & Wood-Harper, A. (1998) Diversity in Information Systems Action Research Methods. *European Journal of Information Systems, 7*(2), 235-246.

Bies, R. and Moag, J. (1986) Interactional Justice: Communication Criteria. In R. Lewicki., B. Sheppard., and M. Bazerman (Eds.), *Research on Negotiations in Organizations* (Vol. 1, pp. 43-55). Greenwich, CT: JAI Press.

Bies, R. and Tripp, T. (1996) The Many Faces of Revenge: The Good, the Bad, and the Ugly. In J. Greenberg and S. Robinson (Chairs), Antisocial Behavior in Organizations. *Research Theory and Applications*. Symposium Conducted at the Annual Meeting of the Academy of Management, Cincinnati, OH. August 1996.

Campbell, M. (1988) Ethics and Computer Security: Cause and Effect. *Proceedings of the 1988 ACM Sixteenth Annual Conference on Computer Science*. Atlanta, Georgia. United States.

Cardinali, R. (1995) Reinforcing Our Moral Vision: Examining the Relationship Between Unethical Behaviour and Computer Crime. *Work Study, 44*(8), 11-17.

Cohen-Charash, Y. and Spector, P (2001) The Role of Justice in Organizations: A Meta-Analysis. *Organizational Behavior and Human Decision Processes*, 86(2), 278-321.

Colquitt, J. (2001) On the Dimensionality of Organizational Justice: A Construct Validation of a Measure, *Journal of Applied Psychology*, 86(3), 386-400.

Colquitt, J., Conlon, D., Wesson., Porter., C. and Ng, K. (2001) Justice at the Millenium: A Meta-Analytic Review of 25 years of Organizational Justice Research. *Journal of Applied Psychology*, *86*(3), 425-445.

Comer, M. (1998) *Corporate Fraud* (3rd ed.). Vermont. Gower.

Cook, P. (1982) Research in Criminal Deterrence: Laying the Groundwork. In N. Morris and M. Tonry (Eds.), Crime and Justice: An Annual Review of Research (Vol. 2, pp. 211-268). Chicago: The University of Chicago Press.

Deloitte. (2006) Global Security Survey.

Deutsch, M. (1975) Equity, Equality, and Need: What Determines Which Value Will Be Used as a Basis for Distributive Justice? *Journal of Social Issues*, *31*(3), 137-149.

Eskew, D. (1993) The Role of Organizational Justice in Organizational Citizenship Behavior, *Employee Responsibilities and Rights Journal*, *6*(3), 185-194.

Essinger, J. (1990) Computer Security in Financial Organizations. Oxford. Elsevier Science Publishers Ltd.

Forcht, K. (1992) Bolstering your Computer's Immune Systems, Security Management, 36(9), 134-140.

Giacalone, R., Riordan, R. and Greenberg, J. (1997) Employee Sabotage: Toward a Practioner-Scholar Understanding. In R. Giacalone and Greenberg, J. (Eds.), *Antisocial Behavior in Organizations*, 109-129. Thousand Oaks, CA: Sage.

Greenberg, J. (1990a) Organizational Justice: Yesterday, Today and Tomorrow, *Journal of Management, 16*(2), 399-432.

Greenberg, J. (1990b) Employee Theft as a Reaction to Underpayment Inequity: The Hidden Cost of Pay Cuts. *Journal of Applied Psychology*, *54*(1), 81-103.

Greenberg, J. (1993) The Social Side of Fairness: Interpersonal and Informational Classes of Organizational Justice. In R. Cropanzano (Ed.), *Justice in the Workplace: Approaching Fairness in Human Resource Management* (pp. 79-103). Hilldale, NJ: Earlbaum.

Greenberg, L. and Barling, J. (1999) Predicting Employee Aggression Against Coworkers, Subordinates and Supervisors: The Roles of Person Behaviors and Perceived Workplace Factors, *Journal of Organizational Behavior*, 20(6), 897-913.

Harrington, S. (1996) The Effects of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions. *MIS Quarterly, 20*(3), 257-277.

Hoffer, J. and Straub, D. (1989) The 9 to 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review, 30*(4), 35-43.

Lee, J. and Lee, Y. (2002) A Holistic Model of Computer Abuse Within Organizations, *Information Management and Computer Security*, *10*(2), 57-63.

Lee, S., Lee, S-G. and Yoo, S. (2004) An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories, *Information and Management*, *41*(6), 707-718.

Leventhal, G. (1976) The Distribution of Rewards and Resources in Groups and Organizations. In L. Berkowitz and W. Walster (Eds.), *Advances in Experimental Social Psychology* (Vol, 9, 91-131). New York: Academic Press.

Leventhal, G. (1980) What Should be Done With Equity Theory? In K. Gergen., M. Greenberg. and R. Willis (Eds.), *Social Exchange: Advances in Theory and Research* (pp. 27-55). New York: Plenum.

Leventhal, G., Karuza, J., and Fry, W. (1980) Beyond Fairness; A Theory of Allocation Preferences. In G. Mikula (Ed.), *Justice and Social Interaction* (pp.167-218). New York: Springer-Verlag.

Mathiassen, L. (2002) Collaborative Research Practice. *Information, Technology & People, 14*(4), 321-345.

Nowakowski, J. and Conlon, D. (2005) Organizational Justice: Looking Back, Looking Forward, *The International Journal of Conflict Management, 16*(1), 4-29.

Parker, D. (1981) *Computer Security Management*, Reston, VA: Reston Publishing.

PwC/CSO/CIO (2008) The Global State of Information Security.

PwC/UK DoBERR (2008) Information Security Breaches Survey.

Rapoport, R. (1970) Three Dilemmas of Action Research. *Human Relations, 23*(6), 499-513.

Shapiro, D., Buttner, E. and Barry, B. (1994) Explanations: What Factors Enhance Their Perceived Adequacy? *Organizational Behavior and Human Decision Processes*, 58, 346-368.

Skarlicki, D. and Folger, R. (1997) Retaliation in the Workplace: The Role of Distributive, Procedural and Interactional Justice, *Journal of Applied Psychology*, 82, 434-443.

Skarlicki, D., Folger, R. and Tesluk, P. (1999) Personality as a Moderator in the Relationship Between Fairness and Retaliation, *Academy of Management Journal*, 42, 100-108.

Sherizen, S. (1995) Can Computer Crime be Deterred? *Security Journal, 6*, 177-181.

Siponen, M. and Iivari, J. (2006) Six Design Theories for IS Security Policies and Guidelines, *Journal of the Association for Information Systems*, 7(7), 445-472.

Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J. (2004) Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. Proceedings of the Tenth Americas Conference on Information Systems, New York, USA.

Straub, D. (1990) Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255-276.

Straub, D., Carlson, P., & Jones, E. (1992) Deterring Highly Motivated Computer Abusers: A Field Experiment in Computer Security. In G. Gable, & W. Caelli (Eds.), *IT Security: The Needs for International Cooperation* (pp. 309-324). Amsterdam: Elsevier Science Publishers.

Straub, D., & Nance, W. (1990) Discovering and Disciplining Computer Abuse in Organisations: A Field Study, *MIS Quarterly 14*(1), 45-60.

Straub, D., & Welke, R. (1998) Coping With Systems Risks: Security Planning Models for Management Decision Making, *MIS Quarterly 22*(4), 441-469.

Susman, G., and Evered, R. (1978) An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly, 23*(4), 582-603.

Tepper, B. and Taylor, C. (2003) Relationships Among Supervisors' and Subordinates' Procedural Justice Perceptions and Organizational Citizenship Behaviors, *Academy of Management Journal*, *46*(1), 97-105.

Thibaut, J. and Walker, L. (1975) *Procedural Justice: A Psychological Perspective*. Hillsdale, NJ: Erlbaum.

USSS/CERT (2005) Insider Threat Study: Computer Systems Sabotage in Critical Infrastructure Sectors.

UK National High Tech Crime Unit (2005) Hi-Tech Crime: The Impact on UK Business.

Walster, E., Walster, G. and Berscheid, E. (1978) *Equity: Theory and Research*. Boston: Allyn & Bacon.

Willison, R. (2002) *Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank*. Unpublished PhD thesis. University of London.

Willison, R. (2006) Understanding the Perpetration of Employee Computer Crime in the Organisational Context, *Information and Organization*, *16*(4), 304-324.

Willison, R. (2006a) Understanding the Offender/Context dynamic for Computer Crimes, *Information Technology & People*, 19(2), 170-186.

Willison, R., and Backhouse, J. (2006) Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective. *European Journal of Information Systems*, *15*(4) 403-414.

Willison, R. and M. Siponen (forthcoming) Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention, Communications of the ACM, Forthcoming.

Workman, M., and Gathegi, J. (2007) Punishment and Ethics Deterrents: A Study of Insider Security Contravention, *Journal of the American Society for Information Science and Technology 58*(2), 212-222.