Abstract

The extant literature analyzing information system security policy violations has primarily focused on accidental or non-malicious noncompliance behavior. The focus is typically on the direct antecedents of behavioral intention, and researchers have applied theories related to planned behavior, adoption, protection motivation, and other cognitive processes. But another class of violation demands greater research emphasis – the intentional commission of computer security policy violation, or computer abuse. Whether motivated by greed, disgruntlement, or other psychological process, this act has the greatest potential for loss and damage to the employer. We argue the focus must include not only the act and its immediate antecedents, but also the cognitive processes leading to the formation of abuse intention, including the motivations and decision processes that may lead up to intention. By presenting three specific examples of how the organization can expand its zone of control further back in time (“to the left of bang”), our framework extends the Straub and Welke (1998) security action cycle. We present the Extended Security Action Cycle, a new theoretic model for illustrating potential organizational impacts on the formation of
employees’ intention to commit computer abuse within the organization. Implications for practitioners and academic researchers are presented, including guidelines for establishing trust with employees that will foster positive perceptions of organizational justice.

**Information System Security Threats**

IS security practitioners are responsible for ensuring the security and privacy of the enterprise information resources by establishing policies, procedures, and practices that preserve the confidentiality, integrity, and accessibility of those resources (widely known as the “CIA Model”). Chief among the functions of security management is the need to address a wide range of threat vectors to be identified and mitigated. Threats to information system security originate from sources that are within the organization itself (internal) or from external vectors, and they may be from human perpetrators or non-human phenomena (Loch, Carr and Warkentin, 1992). We extend the Loch, et al. Threat Taxonomy to include greater granularity, especially for the “insider threat.” See Figure 1.
Internal sources of threat from human perpetrators are the focus of our work and of a growing body of behavioral research within the Information Systems academic discipline (Warkentin and Willison, 2009; Mahmood, Siponen, Straub, and Rao, 2008).

Internal human threats can be entirely passive and non-volitional, such as accidental entry of incorrect data values, which can threaten data integrity, or the actions of employees who are simply careless, sloppy, unmotivated, or poorly trained. Other actions by employees might include volitional behaviours that are not motivated by malicious intentions. For example, individuals who fail to shred sensitive documents, fail to encrypt data before transport it, fail to change passwords, or fail to select strong passwords may knowingly be violating security policies, but not with the intent of inflicting specific harm on the enterprise or its information resources. The third category is the primary focus of our investigation, namely malicious computer abuse by insiders. Passive or benign insiders may violate information system policies with benevolent intent, and the result may be negative, but is often minimally damaging.

(adapted from Loch, Carr, and Warkentin, 1992)
The threat from these accidents by careless individuals is typically dwarfed by the threat from malicious insider computer abuse.

While attempts to gain accurate statistics on employee computer crime are seriously hamstrung by organisational under-reporting due to fears of reputation damage, security surveys provide some indication of the problem. The UK National High Tech Crime Unit (2005) reported that 38% of financial fraud, 68% of theft of information/data, and 100% of 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 worrisome data. The PricewaterhouseCoopers/UK Department for Business Enterprise and Regulatory Reform survey (PwC/DoBERR, 2008) notes that for large organizations (250+ employees), 57% of respondents reported the cause of their worst security incident to be internal, and the Global State of Information Security survey (PwC/CSO/CIO, 2008) showed that employees (former and current) formed the biggest threat for respondents. In a recent survey of IT security professionals, insider misuse and unauthorized access to information by insiders are the No. 1 and No. 2 security threats overall (Carr, 2007), ahead of malware, hackers, and other IS security threats. The respondents expressed concerns about “violation of the organization’s policies regarding acceptable use of computing/network resources.”

The IS security community has responded to these concerns about insider abuse by undertaking a large number of studies which have examined the issue of compliance or noncompliance with policies. As Figure 1 portrays, These studies have largely focused on the behavior of honest employees and examined factors which either hinder or facilitate compliance with security policies (Bulgurcu, Cavusoglu and Benbasat, 2010; Johnston and Warkentin, 2010; Siponen and Vance, 2010; Boss et al., 2009; D’Arcy, Hovav and Galetta, 2009; Herath and Rao, 2009; Lee and Larsen, 1990; Myyry et al., 2009, Workman, Bommer and Straub, 2008; Pahnila, Siponen and Mahmood, 2007; Dodge, Carver and Ferguson, 2007; Sasse, Brostoff and Weirich, 2001; Straub, 1990). In Figure 1, these violations generally fit with the volitional, but non-malicious actions of employees. Such violations typically represent a small cost
to the enterprise. But there is also the need to consider the motivation and behavior of those intent on committing some form of computer crime, especially give the much greater potential cost of such computer abuse. It is perhaps surprising, therefore, that a focus on understanding offender behavior has received far less attention in the IS security field (Warkentin and Willison, 2009).

We argue that a greater emphasis on understanding the intentional offender’s thought processes and behavior will not only assist in enhancing existing research subject areas, but will also present original avenues for future research. In addition, with this emphasis, it is possible to extend the traditional areas of safeguard implementation depicted by Straub and Welke’s (1998) widely cited and well established Security Action Cycle (see Figure 2). Central to their model are four areas of implementation which include deterrence, prevention, detection and remedies. The aim of these four areas is to enhance IS security by reducing risk to systems. Hence, organizations would first attempt to address the risks posed by the insider by deterring potentially dishonest staff. If this fails, preventive measures would aim to stop the commission of computer crime, followed by efforts targeted at detection, and finally the pursuit of remedies (see Figure 2).
Importantly, Straub and Welke (1998) argued that organizations must attempt to maximize deterrence and prevention efforts, while minimizing the need for ‘detection’ and ‘remedy.’ While deterrence might be considered the first line of defense for organizations, we suggest that a focus on the intentional offender allows recognition of “pre-kinetic events” to the left of this ‘line,’ thereby extending the zone of control for organizations and increasing the options for safeguard implementation that are available to them (See Figure 3). Such a model would offer organizations the ability to maximize attempts to subvert employee computer crime, as opposed to falling victim to it.

Figure 3 illustrates the focus of this paper on the “pre-kinetic” events (to the “left of bang”) that precede and contribute to the motivation of individual employees to commit malicious computer security policy violations or computer abuse.
In the subsequent sections, we will address both the extant literature related to the problem of insider computer abuse and the precise nature of this phenomenon from the psychological perspective of the insider himself. The thematic development will be established on the foundations of the literature as well as on the paradigm of this psychological process that precedes the actual perpetration of computer abuse. If an organization can influence the process that leads to employee motivation which, in turn, leads to the formation of behavioral intention to commit an act of computer security violation or a crime, it may reduce the frequency and severity of such crimes, and therefore may reduce the tremendous costs incurred by these breaches. While we do not claim that our thematic development is exhaustive, we do believe it illustrates the potential for focusing on the offender in this manner.

Current Research in IS Security Violations

In the following sections, we review the extant research literature which addresses the thought processes and behavior of the individual who is a potential or actual criminal
offender in the information systems environment, while focusing specifically on the insider or organizational employee. We start with literature addressing the actual perpetration, then move backward along the timeline. We look at the prevention of the offense, and then we discuss the studies on factors leading to the formation of behavioral intention to commit an offense, followed by a review of the deterrence literature. We conclude the review by examining the work on offender motivation, which may occur even earlier along the timeline. Consistent with our main argument, we have structured the literature review so that each section represents a move to the left of the ‘commission’ of the crime along the timeline.

Prevention

Immediately before an intentional violation occurs, an organization can use a variety of measures designed to prevent the abuse. These include network traffic scanning, authentication systems, physical (facility and computer) security, and other technical controls. Willison (2002) and Willison and Backhouse (2006) have examined the issue of prevention from the offender’s perspective by examining criminal opportunity. More specifically, they advanced a model known as the ‘Crime Specific Opportunity Structure.’ Drawing on a number of criminology theories, the model encapsulates those factors which are believed to offer an opportunity for computer abuse prevention. Willison and Backhouse (2006) argued that the model can improve managers’ knowledge of systems risk and thereby help to enhance safeguard

---

1 This focus on moving “to the left” is inspired in part by so-called “fourth-generation military strategy,” which has identified the need to focus “left of bang” in an effort to stop the formation of aggressor intention long before an act of military aggression occurs. In the words of one military leader, “...security is, at its core, a thinking-man’s game where intellect borne of training and experience ought to be the most prized commodity. Those who are trained to do so can design security systems ... that mitigate risk in the first place and thus avoid [violations] in many cases. In military jargon this is often called pre-kinetic or left-of-bang, meaning they are the actions taken long before an incident occurs. This is perhaps the most important and certainly the most underrated aspect of security [management].” (Allen, 2009). Proponents argue that managers must act “proactively, left-of-bang, before only kinetic options remain.” (Clarke, 2009). Similarly, military strategists now speak of “winning the hearts and minds of the population,” similar to the way that organizations may seek to psychologically influence employees long before computer abuse or security violations occur.
implementation. While the aforementioned work considers the structure of opportunities, Willison (2006) and Willison and Siponen (2009) have examined the process of perpetration in the organizational context. These papers proposed the use of *crime scripts* for understanding how offenders interact in specific environments during the commission of computer abuse. As any crime is made up of a series of stages, these scripts allow for the consideration of offender behavior at each of these stages and in terms of the context in which the computer abuse takes place. It is argued that a clearer understanding of offender behavior provides greater insights with regard to the implementation of preventive countermeasures.

**Intention**

Moving further to the left along the timeline of the offender’s psychological process, an organizational can seek to interrupt the formation of actual intention to commit the act of computer abuse. Researchers have combined a number of theories in order to understand the formation of offender behavioral intention (Foltz, 2000; Lee and Lee, 2002; Lee et al, 2004; Workman and Gathegi, 2007).

Lee et al (2004), for example, used the Theory of Planned Behavior for an overarching framework, and drew on General Deterrence Theory (GDT) and Social Control Theory (SCT), for examining intention. A key aspect of GDT is the role played by sanctions (Cook, 1982), in terms of their perceived certainty and severity by the offender. If an offender perceives the certainty of being caught as high, and if he believes the associated sanctions will be severe, then the offender will be deterred (Straub, 1990). Social Control 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 behavior. Lee et al. (2004) focused on two groups of factors which they believed influenced two forms of intention termed self-defense and induction control. In consequence, security policy, security awareness, and security system were thought to impact on self-defense intention by acting as deterrent factors. In addition, the four factors addressed by Social Control Theory, which create a social bond, were equated by Lee et al. as organizational trust. Hence, the social bond (level
of trust) between an individual and the organization in which they work were thought to influence the induction control intention. In their sample of Korean managers, Lee et al. (2004) found security system to be a positive deterrent factor, while involvement and norms (acting as organizational trust factors) positively influenced induction control intention.

Deterrence

The issue of deterrence has been addressed by several IS security researchers, and represents, by far, the must studied area of employee computer crime (Campbell, 1988; Cardinali, 1995; Harrington, 1996; Hoffer and Straub, 1989; Sherizen, 1995; Straub, 1990; Straub and Nance, 1990; Straub and Welke, 1998). Perhaps not surprisingly, a number of scholars 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; D’Arcy and Hovav, 2007). D’arcy et al. (2009), for example, examined how the perceived certainty and security of organizational sanctions, influenced IS misuse intentions. Unlike other studies, however, their research represented a departure by examining how these perceptions were influenced by user awareness of three forms of security countermeasures. These included i) user awareness of security policies, ii) security education, training, and awareness, iii) and computer monitoring. On the whole, these countermeasures were positively associated with perceived certainty and severity, though this was not the case with regard to policies and perceived certainty. In terms of the sanctions, the results revealed that perceived severity would be more effective in reducing misuse than perceived certainty. Interestingly, further analysis revealed that moral commitment moderated both impact of certainty and severity on misuse intention.

Offender Motivation

Computer abusers, including insiders are often driven by various motivations, which may be the result of managerial or organizational actions. The issue of motivation has rarely been addressed in the IS security field. However, Straub (1990) examined the extent to which deterrents and rival explanations were related to levels of computer
abuse. Rival explanations included motivational, environmental (“tightness of the security environment and visibility of security administrators”) and preventives (physical and software security) factors. Specifically, motivational factors included system privileges, the strength of offender motivation, the extent of offender collusion and employment status. Straub assessed these factors in relation to incidents of abuse reported by survey respondents. Hence, 259 cases were noted in a sample of 1,211 questionnaires. Overall, the data indicated that deterrents (along with preventives) were effective in lowering incidents of abuse, while rival explanations were generally insignificant.

More recently, Shropshire (2009) focused on cases of sabotage and espionage, by rogue employees. In particular, the relationships between the employees’ background/motives and the specific crimes were explored. Using canonical analysis, 62 cases were examined in relation to the independent variables of financial-changes, relationship-issues, substance-abuse and job-changes. The analysis indicated significant latent structures between the independent and the dependent (sabotage/espionage) variables. The research discovered that cases of espionage were highly correlated with financial changes followed by relationship changes, while incidents of sabotage were most highly correlated with job changes, then substance abuse and relationship changes.

The reviewed literature has proved insightful and provided a firm basis for additional research into insider threats. We, however, believe that a specific focus on the cognitive processes of the offender can not only assist in enhancing existing research areas, but also present original avenues for future research. This enables consideration of phenomena to the left of deterrence and, by so doing, opens up new areas for safeguard application. As a consequence, the zone of control for organizations may be expanded. The following three sections of the text provide three specific examples of how organizations may extend their ability to influence the thought processes of insiders who may commit computer abuse. The first focuses on individuals’ moral justification process, and the related techniques of neutralization. The second addresses expressive and instrumental motives for computer abuse. And the final area explores the role of perceptions of organizational justice and injustice in
establishing the motivation to commit computer abuse against the organization. Following each are a series of research questions for future consideration.

Process 1. Criminal Justifications and Deterrence

The first illustration focuses on offender deterrence. As already discussed, the existing IS security studies have addressed how external factors (e.g. security awareness and monitoring of networks) may reinforce offender perceptions of certainty and severity. However, theory and research from the fields of psychology and criminology have also indicated that individuals embody ‘self-deterring’ mechanisms (Bandura et al., 1996) and ‘internalized norms’ (Sykes and Matza, 1957) which influence decisions to engage in criminal behavior. That said, authors from these two fields have also noted that individuals can employ ‘mechanisms of moral disengagement’ (Bandura et al., 1996) and ‘techniques of neutralization’ (Sykes and Matza, 1957) for helping to dissipate internalized norms and social censure (i.e. the ‘self-deterring’ mechanisms). This allows the offender to engage in a criminal act without feelings of guilt and shame. By considering how to negate these ‘mechanisms’ and ‘techniques’, this would provide an additional focus and area for pursuing deterrence in the organizational context. The relevant literature from the fields of criminology and psychology will now be discussed in detail.

Techniques of Neutralization

In their seminal text Sykes and Matza (1957) rejected the idea of a delinquent sub-culture in which the prevailing values represent an inversion of those held by respectable society. The subsequent paradoxical question addressed by Sykes and Matza is why does delinquency occur if there is a commitment to the ‘usages of conformity’? The authors argued that much delinquency is ‘justified’/rationalized in a manner which negates the ‘disapproval flowing from internalized norms and conforming others in the social environment’. Hence, these social controls and internalized norms, which keep in check and restrain criminal behavior are ‘neutralized’, leaving the delinquent free to offend. Given this, Sykes and Matza termed these justifications ‘techniques of neutralization’ and advanced five types. See
Appendix A for a description of these techniques, which include denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and the appeal to higher loyalties. So, for example, with regard to the denial of the victim:

Even if the delinquent accepts the responsibility for his deviant actions and is willing to admit that his deviant actions involve an injury or hurt, the moral indignation of self and others may be neutralized by an insistence that the injury is not wrong in light of the circumstances. The injury, it may be claimed, is not really an injury; rather, it is a form of rightful retaliation or punishment. By a subtle alchemy the delinquent moves himself into the position of an avenger and the victim is transformed into a wrong-doer (Sykes and Matza, 1957, p. 668).

As a theory, the techniques of neutralization have been readily embraced in the field of criminology to address a diverse range of deviant or criminal behavior (see Maruna and Cope, (2005) for an extensive review). These have included, for example, shoplifting (Cromwell and Thurman, 2003), poaching (Eliason and Dodder, 1999), corporate crime (Piquero et al. 2005), white-collar crime (Benson, 1985), tax evasion (Thurman, 1984), drug abuse (Priest and McGrath, 1970), car theft (Copes, 2003), and domestic violence (Dutton, 1986). Given the popularity of this theory, aside from its application, a number of researchers have advanced other techniques of neutralization which could be employed in criminal behavior. These authors include Klockars (1974) (‘metaphor of the ledger’), Minor (1981) (‘defense of necessity’), Coleman (1994) (‘defense of the necessity of the law’ and ‘claim of entitlement’), Henry and Eaton (1994) (‘claim of normalcy,’ ‘denial of negative intent,’ and ‘claim of relative acceptability’), Cromwell and Thurman (2003) (‘claim of postponement’ and ‘claim of individuality’), and Garrett et al. (1989) (‘avoidance of greater harm,’ ‘legal rights,’ ‘comparative standards,’ and ‘malicious intentions’).

Mechanisms of Moral Disengagement

Criminology is not the only field which has considered how criminal behavior is justified by the offender. The renowned psychologist, Albert Bandura, has written extensively on this topic (Bandura, 1986; Bandura et al., 1996; Bandura, 1999; Bandura, 2002). He argued that the regulation of human conduct requires more than
moral reasoning for it to occur. What a theory of moral agency also needs is an explanation of the relationship between moral reasoning and moral conduct. Hence, Bandura advanced an “agentic theory” of morality which moves beyond a focus on cognitions about morality. In his social cognitive theory of the moral self, therefore, Bandura explains the link between moral reasoning and moral action through “affective self-regulatory mechanisms.”

As an individual develops a moral-self, standards of right and wrong are adopted, which act as a guide and crucially with regard to our concerns, act as a deterrent for conduct. Through the process of self-regulation, individuals monitor their behavior in specific contexts, and judge it in relation to moral standards and the perceived circumstances. The individuals’ behavior is consequently regulated based on their judgments. Bandura claimed that individuals pursue behavior which provides a sense of self-worth and satisfaction at the expense of alternative actions which could breach moral standards. Such a breach could further lead to self-condemnation in the form of negative self-sanctions. The use of negative sanctions to curtail violations of moral standards, and positive sanctions for actions more aligned with moral standards, operate in anticipation of the said behavior. Given situational inducements which could lead to inhumane actions, an individual can choose more appropriate behavior, through self-influence in the form of self-sanctions.

Of some significance, Bandura argued that self-regulatory mechanisms will only operate if they are activated. In addition, he advanced a number of “psycho-social maneuvers” which disengage moral self-sanctions from inhumane conduct. These allow people with the same moral standards to act differently owing to the selective activation and deactivation of these sanctions. Specifically, Bandura termed these psycho-social maneuvers mechanisms of moral disengagement (see Appendix A for a description of these mechanisms). These include ‘moral justification,’ ‘euphemistic labeling,’ ‘advantageous comparison,’ ‘displacement of responsibility,’ ‘diffusion of responsibility,’ ‘disregarding or distortion of consequence,’ ‘dehumanization,’ and ‘attribution of blame.’ So for example, with regard to displacement of responsibility, Bandura et al. (1996: 365) observed:
Self-sanctions are actively most strongly when personal agency for detrimental effects is acknowledged … Under displacement of responsibility people view their actions as springing from the social pressure or dictates of others rather than as something for which they are personally responsible (Andrus, 1969). Because they are not the actual agents of their actions, they are spared self-censuring reactions. Hence, they are willing to behave in ways they normally repudiate if a legitimate authority accepts responsibility for their actions.

It has been noted in the literature that our understanding of moral disengagement for explaining unethical behavior is still at an early stage (Detert et al, 2008; Moore, 2007). Early work in this area has focused on the aggressive and anti-social behavior of children (Bandura et. al., 1996; Bandura et al., 2001; Mensini et al., 2003). However, more recent research has addressed adult behavior with regard to drug abuse (Barnes et al., 2005), undesirable civic behavior (Caprara and Capanna, 2006), delinquency (Kiriakidis, 2008), and advocacy of aggressive militaristic actions (Aquino et al., 2007; McAlister, 2001).

IS Research and Rationalizations

As discussed, these two bodies of theory, particularly the techniques of neutralization, have been applied to research diverse forms of criminal/deviant behavior. Given this, it is perhaps no surprise to learn that these forms of behavior have recently encompassed IS related areas. These forms of behavior include cyber-loafing (Lim, 2002; Lim and Teo, 2005), digital piracy (Hinduja 2007; Ingram and Hinduja, 2008; Morris and Higgins, 2009), and non-compliance to information security policies (Siponen and Vance, 2010). While Siponen and Vance’s (2010) study acts as a contribution to the compliance literature, earlier IS security work has considered how dishonest employees

Research Question 1: Which rationalizations are associated with particular forms of employee computer crime/deviance?

A starting point would be to identify which rationalizations (if any) are associated with particular forms of employee computer crime/deviance? Although Sykes and Matza (1957) argued that specific neutralizations may be more suited to particular deviant acts, even the most recent literature has indicated the need to make progress in this area (Ingram and Hinduja, 2008; Maruna and Copes, 2005).

Research Question 2: Does the seriousness of a criminal act impact the application of rationalizations?

Maruna and Copes (2005) noted that some researchers believed the techniques of neutralization offer an understanding into participation with regard to minor forms of crime and delinquency, but provide little explanation when addressing more serious criminal behavior (Mitchell and Dodder, 1980, 1983). Is this the case with regard to employee computer crime/deviance? Lim’s research (Lim, 2002; Lim and Teo, 2005) indicates how employees rationalize their behavior in terms of the relatively minor deviant act of ‘cyber-loafing’, but what about more serious instances of computer fraud or sabotage?

Research Question 3: Is there a curvilinear relationship between rationalizations and computer crime/deviance?

Related to the seriousness of the offence is the degree of commitment by the offender to crime. Recent research has indicated that the relationship between rationalizations and crime/deviance is curvilinear (Copes and Williams, 2007; Maruna and Copes, 2005; Ingram and Hinduja, 2008). Hence, those individuals who feel the need to invoke neutralization techniques and justify their behavior may only be partly committed to criminal behavior. This is in contrast to those who are either completely committed to criminal behavior or completely committed to conventional conforming behavior. Either way, it is argued that the two groups would not feel the need to rationalize their behavior. Support for this argument is provided by Ingram and Hinduja (2008) in their study of music piracy. They found that neutralizations were
most applied by those who only perpetrated moderate amounts of piracy, and were less relevant for those who committed 'high' levels. Interestingly, this mirrors the argument advanced by Chambliss (1967), who argued that with regard to deterrence, those totally committed to a criminal lifestyle would not be influenced by deterrence. Similarly, for those who were totally committed to the norms of conventional society would pay no regard to deterrence sanctions, given their non-criminal lifestyle.

**Research Question 4:** What moderators influence the rationalization process?

Identifying those factors which moderate the influence of rationalizations also represents an area for future research. Agnew’s research (Agnew and Peter’s, 1986; Agnew, 1994), for example, identified the role of an individual’s belief system. He argued that an individual may engage in criminal/deviant actions, even though they may disapprove of such activities. Therefore, neutralizations would be invoked to justify their actions, and once this is achieved, this brings the individuals actions in line with their beliefs. Supporting evidence for this argument was recently provided by Ingram and Hinduja’s (2008) research into music piracy.

Other moderators which could be studied include situational factors. Earlier research has indicated that rationalizations would not be invoked unless a situation allows this to happen (Sykes and Matza, 1957; Matza, 1964; Agnew and Peters, 1986; Agnew, 1994). Angew (1994: 562), writing about delinquency, argued that:

```
‘… at a minimum, neutralization will not lead to delinquency unless adolescents also believe they are in situations in which the neutralizations are applicable. For example, adolescents who believe that fighting is justified in response to insult will not turn to fighting unless they also believe they have been insulted’.
```

This argument is consistent with later research by Lim (2002). In her study of cyberloafing, she found that when employees perceive that they have been treated unfairly, in response they evoke the metaphor of the ledger (Klockars, 1974). Therefore, future research could consider if a context must provide a particular reason (e.g. a feeling of injustice) for a rationalization to be evoked. Without such a reason, will rationalization still be used?
Process 2. Motives and Deterrence

Our next opportunity for extending the organization’s zone of control focuses on the relationship between the motive of the crime and the ability to deter the offender. It has largely been assumed within the IS security field that all forms of computer crime, irrespective of motive or type of crime, can be deterred. However, there is little empirical evidence from the field of criminology to support this assumption (Nagin, 1998). Indeed, drawing on the relevant literature, we illustrate how the issue of motive may influence the extent to which deterrence is possible. Further research is required to address this issue, but for now, we will argue why we believe this to be the case. To do this, we first draw from the field of criminology, and consider crimes in terms of their instrumental or expressive motives.

Instrumental crimes (Ekblom, 1997; Burek, 2006) focus on achieving a goal where the criminal act is viewed as a means to an end. For example, an offender may perpetrate a mugging with the intention of acquiring money. Hence, in this example, the mugger commits the crime because it is instrumental to the achievement of the goal i.e. acquiring cash. Expressive crimes often involve frustration, anger, rage and despair. Unlike instrumental offences, the actual commission is considered an end in itself (Ekblom, 1997; Burek, 2006) and there is no additional goal to be met. Cases of aggravated assault, for example, may involve the resolution of anger issues. While expressive crimes can lack premeditation, it has also been noted how offences in this category (e.g. hate crimes) can involve a degree of planning.

The instrumental/expressive distinction has been used by criminologists to address a diverse range of crimes including terrorism (Amir, 1988), rape (Prentky et al, 1985; Rosenberg et. al. 1988), vandalism (Whittingham, et. al. 1999), workplace violence (Swanton, 1989), intra-family violence (Gelles, 1987; Dawson, 2006), arson (Fritzon, 2001; Hakkanen, et. al. 2004) and violent street-crime (Bennett and Brookman, 2008). It is, however, important to note that specific crime types cannot simply be classified as either ‘instrumental’ or ‘expressive’. Homicide is a case in point, whereby this form of offence can be categorised along instrumental or expressive lines (Polk, 1994; Block and Christako, 1995). Brawls and arguments, for example, which result in...
homicide, are typically classified as expressive, as the violence associated with the killing is the dominant motive (Santtila et. al., 2003; Miethe and Drass, 1999; Salfati, 2000; Polk, 1994). Other homicides are classified as instrumental because the killing of an individual can be considered a ‘side-effect’ of the pursuit by the criminal of a primary goal (Maxfield, 1989). Empirical research in this area has indicated how robbers convicted of homicide, have perpetrated murder in pursuit of the instrumental goal e.g. money.

Deterrence and Expressive Motivations

For this paper, the greatest significance of the distinction between expressive and instrumental motives concerns the implications for deterrence. More specifically, authors within the field of criminology have argued that deterrent sanctions apply most readily to crimes with instrumental motives, whereas offences driven by expressive ones are considered harder to deter (Chambliss, 1967; Parker and Smith, 1979; Thomas and Williams, 1977). Of the authors who have questioned the ability to deter expressively motivated crimes, the most well known is probably Chambliss (1967). He argued that the efficiency of deterrence is dependent on two factors. First, if the crime is either ‘instrumental’ or ‘expressive’ in nature, and secondly, whether an individual has a low or high commitment to crime. Combining these two distinctions, Chambliss argued that those who have a low commitment to crime and perpetrate instrumental offenses are most likely to be deterred, while those with a high commitment and undertake expressive criminal acts are least likely to be deterred. In relation to the other two types, he noted (Chambliss, 1967: 713).

While we can assert with some confidence that the remaining two types – high commitment/instrumental and low commitment/expressive – will fall between the two polar types, it is somewhat more difficult to know which of those types will be more responsive to punishment. It seems likely, however, that the impulsive nature of expressive acts, even when commitment is low, will make such acts less amenable to punishment than instrumental acts, even though the commitment is high.

Whatever the merits, and despite the age, of the arguments advanced by Chambliss, it is important to note that the deterrence literature has not resolved the issue of whether
expressive based crimes are less deterrable than instrumental offences. Nagin (1998) addressed why this is the case in his paper ‘Criminal Deterrence Research at the Outset of the Twenty-First Century’ and pointed to four significant gaps in knowledge between sanctions policy and deterrence efficacy. Of specific relevance to the current paper concerns the knowledge gap regarding the relationship between sanction policy and offender perceptions of certainty and severity. In providing some background to his arguments, Nagin noted how three ‘largely disconnected’ bodies of research have evolved in the deterrence literature. These include interrupted time-series, ecological, and perceptual deterrence studies. The first of these examine specific and targeted interventions e.g. a police crackdown on an area known for drug dealing (Sherman, 1990). Ecological studies focus on sanction levels across time and space and how these influence crime rates (e.g. Samson and Cohen, 1998; Levitt, 1996). Finally, perceptual deterrence research examines offenders’ perceptions of certainty/severity and self-reported crime (Grasmick and Bursick, 1990; Paternoster and Simpson, 1997). This body of research emerged owing to the realization that deterrent affects ultimately occur through perceptions of certainty and severity. In addition, impetus was given to this area of research through doubts that actual and perceived sanction threats were closely linked.

While Nagin argued that deterrent effects have been identified in all these three areas of research, he also acknowledged the paucity of empirical research with regard to how sanctions impact offender risk perceptions i.e. perceptions of certainty and severity. With regard to interrupted time-series and ecological studies, their focus has been on the link between sanction policy and crime i.e. actual criminal behavior. As a consequence, the intervening relationship between sanctions policy and offenders’ perceptions of certainty and severity has been left as a ‘black box’. Somewhat surprisingly, given the doubts by perceptual deterrence researchers over the extent to which actual and perceived threats are closely linked, even this group of writers have given only ‘modest attention’ to the manner in which risk perceptions are formed. Consequently, as Nagin argued, this leads to a knowledge gap concerning the etiology of deterrence.
However, this oversight has also occurred in our own field. IS security researchers have not yet considered the relationship between sanctions policy and sanction perceptions. This is problematic because the relationship between sanction policy and offender perceptions plays an implicit, but integral role in the relationship between sanction policy and offender behavior. As noted, it is the offender’s perceptions of certainty and severity which influence their behavior. However, unless these perceptions can be manipulated by policy, then deterrence will not occur. Therefore, what is needed is a clear understanding of how risk perceptions are formed and influenced. To simply assume that sanctions will always influence behavior is wrong. It may well be, for example, that computer crime, motivated by expressive factors, may be less deterrable than instrumentally motivated offences, but only future research can provide the answers.

Research Question 1: Are risk perceptions of certainty and severity, crime specific or generalized?

With regard to risk perceptions, Nagin (1998) questioned:

‘whether sanction risk perceptions are well formed at the level of the specific offense – for example, burglary versus robbery – or do would be offenders have only a generalized sense of the effectiveness of the enforcement apparatus? For instance, are perceptions of apprehension risk formed principally by broad based impressions of the police being proactive in suppressing disorder, as suggested by Sampson and Cohen (1988) and Wilson and Boland (1978), or are they more crime specific and determined by the rate at which police actually solve specific types of crime?’ (Nagin, 1998: 18)

Nagin argued that the answer to this question has important implications for deterrence policy. Rational choice models of criminal behavior assume that an increase in jail terms for a specific crime, for example, robbery with a firearm, will have the desired affect. That is a drop in the levels of this offence. However, this prediction also assumes that offenders also have separate perceptions of certainty and severity for each specific crime. Or is it the case that offenders’ perceptions of certainty and severity are tied to overall impressions of the ‘effectiveness of the enforcement apparatus?’ This argument also has implications for the way deterrence
actions are enacted in the organizational context. Should organizations implement a targeted crime specific deterrence policy or would this simply lead to enhancing generalized perceptions? Understanding the issue of granularity would assist organizations in deciding how best to organize limited resources.

**Research Question 2**: How are perceptions of certainty and severity formed?

Of key importance would be to address how perceptions of certainty and severity are formed. Specifically, research needs to firmly establish if individuals’ sanction perceptions are influenced by organizational deterrence policy. What factors influence these perceptions? For example, how do individuals become aware of changes in organizational security practices? What informational sources would they use in updating their impressions? How would different forms of enacting deterrent policies affect sanction perceptions? These questions would all assist in understanding the extent to which risk perceptions are manipulated by organizational policy.

**Research Question 3**: What factors moderate the relationship between organizational policy and risk perceptions?

As noted in this section of the paper, aside from considering those factors which may positively reinforce risk perceptions, there is also the need to consider moderating factors. Was Chambliss (1967) correct in arguing that the degree of commitment to crime and the instrumental or expressive nature of the offence influence perceptions of certainty and severity?

**Research Question 4**: What influences the maintenance and decay of sanction perceptions?

Examining the link between policy and perceptions, from a temporal perspective, could form another area for future research. Moving away from studies with a focus on sanctions at a specific point in time, an extension of these studies would explore those factors which influence perceptions of certainty and severity over periods of time.
Process 3. Employee Disgruntlement

If it is found that expressively based crimes are less deterrable, this would mean that the first line of defense for organizations would not be deterrence, but rather prevention. One option, therefore, would appear to involve moving left along the timeline and consider examining the root causes of motivational factors. If substantial gains could be made in mitigating those factors which create motives, then this would substantially extend the zone of control, afforded to organizations. Additionally, if motive could be negated, then the possibility of expressive crimes proving less deterrable would become a non-issue, as an unmotivated individual poses no threat. This section of the text, therefore, addresses the issue of motive through a discussion of workplace disgruntlement. It is believed that an understanding of inroads into the root causes of motivation can be made by equating it with perceptions of fairness/unfairness held by employees in the organizational context.

As noted, there is currently a paucity of material focusing on the area of offender motivations. While external factors are difficult to address (Essinger, 1990; Comer; 1998), we argue that progress may be made in addressing motivational factors by examining the organizational context and the influence it may have on individuals. One area which offers considerable research potential is the phenomenon of workplace disgruntlement. A report, for example, by the US Secret Service and Carnegie Mellon (USSS/CERT, 2005) entitled ‘Insider Threat Study: Computer Systems Sabotage in Critical Infrastructures’, studied forty nine cases of insider sabotage. One of the key findings was that in eighty eight per cent of cases, the perpetrator held a ‘work-related grievance’ before the act of abuse. In addition, another key finding viewed these grievances as a ‘trigger’ for their criminal actions.

Organizational Justice

To address the problem of disgruntlement, we propose the use of an existing body of research, which examines the issue of fairness within the organizational context. This body of research falls under the umbrella term ‘organizational justice.’ There are four main constructs which relate to different organizational phenomena and influence employees’ perceptions of fairness/unfairness in organizations or what is
interchangeably termed justice/injustice. 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 (Willison and Warkentin, 2009). Of great importance is the recognition that as factors within the organizational context create disgruntlement, there at least exists the potential for addressing this problem. 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 may feasibly be introduced to address this problem, for while corporations may rely heavily on controls to deter or prevent employee computer crime, why not mitigate disgruntlement and therefore forestall criminal behavior in the first instance? The four organizational justice constructs will now be described followed by a discussion of their application for addressing employee computer crime.

**Distributive justice**

Seminal work, in this area was undertaken by Adams (1965), who advanced a theory of equity. Adams argued that in terms of distributive justice, individuals compare the ratio of their work outputs (rewards) and inputs (contributions) to the ratio of a comparative other (e.g. a colleague). Central to this comparative process are what Adams (1965) termed ‘normative expectations’ which are learned through socialization in forums such as home, school and work. Crucially, Adams (1965, p. 280) observed that:

> When the normative expectations of the person making social comparisons are violated, when he finds that his outcomes and inputs are not in balance in relation to those of others, feelings of inequity result.

**Procedural Justice**

Original work in this area related not to the organizational, but rather the legal context (Colquitt et al, 2001). Thibaut and Walker’s (1975) ground breaking research in this area led to their own formulation of procedural justice. Using simulated dispute resolution (mediation and adjudication) cases, they examined third-party procedures
and the amount of control afforded disputants over these procedures in terms of ‘process’ and ‘decision.’ The former relates to the amount of control a disputant has over the actual procedures designed to settle grievances, while the latter refers to the degree of control over directly determining the outcome decision. Thibaut and Walker’s (1975) research found that disputants were willing to cede control of the actual decision to a third party as long as they were able to maintain process control. Hence, their research highlighted how process control, or in other words the ability to ‘voice’ an opinion is a central factor with regard to what constitutes procedural justice.

While Thibaut and Walker’s (1975) work focused on the legal context, it was the research of Leventhal and his colleagues (Leventhal, 1980; Leventhal et al, 1980), which first addressed procedural justice in the organizational context. Departing from a focus on process control, Leventhal focused on the nature of the procedures and the implications for procedural justice perceptions. Six rules were identified, which, if followed, it was argued, would lead to the development of fair procedures. As Cohen-Charash and Spector (2001, p.280) noted, these rules included:

- 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 organization, 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 corporate recruitment, therefore, considered interactional justice to comprise of four elements which included 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 (1990, 1993) split interactional justice into two other constructs entitled ‘interpersonal’ and ‘informational’. Greenberg (1990, 1993) viewed 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 (1990, 1993) further asserted 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 noted 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.

In a later study, Shapiro et al. (1994) added to the informational justice literature through their research into factors which influence the perceived adequacy of explanation. As part of their findings, they argued that perceptions of informational justice are enhanced when explanations are considered reasonable and specific i.e. tailored to the individual.

A considerable body of research has addressed the ‘outcomes’ which impact organizations as a consequence of perceptions of justice/injustice (see Colquitt et al (2001), Nowkowski and Conlon (2005) and Cohen-Charash and Spector (2001) for extensive reviews of this literature). While some of the reactions can be considered relatively benign (e.g. employee withdrawal, reduced job satisfaction and declining...
organizational performance), other more extreme responses have included theft (Greenberg, 1990, 1993), retaliation (Skarlicki and Folger, 1997; Skarlicki et al, 1999), revenge (Bies et al, 1997; Bies and Trip, 1998), workplace violence (Greenberg and Barling, 1999) and sabotage (Ambrose et al, 2002; Giacolone et al, 1997). Ambrose et al. (2002), for example, found injustice (unfairness) to be the most frequent cause of workplace sabotage, over other explanations which included powerlessness, frustration, boredom/fun and facilitation of work.

A recent paper by Willison and Warkentin (2009) highlighted an incident of computer sabotage by a disgruntled female DBA. When the forms of organizational justice are applied to the case, it can be seen that the staff member experienced procedural, distributive and possibly even informational injustice. Considering disgruntlement in terms of organizational 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 organizational phenomena, which create the different forms of injustice, and by so doing aids their mitigation. The ability to negate disgruntlement would also be of obvious interest to practitioners, particularly as the organizational justice literature offers the potential to develop a new range of safeguards. So the 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.

**Research Question 1**: Do perceptions of injustice motivate employee computer crime?

An obvious broad area of research to address would be to examine if perceptions of injustice motivate employee computer crime. For individual research studies, a good starting point might be to consider the forms of injustice in relation to specific crimes. For example, Skarlicki and Folger (1997) explored the relationship between retaliation in the organizational context and perceptions of distributive, procedural and interactional justice. Hence, studies in the IS security field could equally examine forms of computer crime in relation to one or all of the forms of organizational justice.
Research Question 2: Does the additive effect of multiple forms of injustice influence the seriousness of an offence?

Future research could also examine the additive effect of the different types of injustice. Studies have indicated that the seriousness of the deviant act increases when individuals experience multiple forms of injustice (Ambrose et al. 2002). This has been described by McLean Parks and Kidder (1994) as the ‘Popeye effect’ as the cartoon character is famed for saying ‘That’s all I can stands, cuz I can’t stands no more’ (McLean Parks and Kidder, 1994: 133).

Research Question 3: Can perceptions of informational and interactional justice moderate perceptions of distributive or procedural injustice?

Moderators of organizational justice also warrant further study. As discussed, the four forms of injustice can have an additive negative effect. However, the right combination of organizational phenomena can also lead to perceptions of fairness. Therefore, even if an employee experiences, for example, distributive injustice, this perception of unfairness can be moderated by perceptions of informational and interactional justice (Greenberg, 1990; 1993). Hence, one area for future research could involve examining the moderating relationship between the forms of injustice.

Conclusion

While numerous studies have focussed on the security behavior of honest employees, little attention has been paid to those employees who perpetrate computer abuse. Whether motivated by greed, disgruntlement, or other psychological process, this act has the greatest potential for loss and damage to the employer. We argue that not only must a focus on the offender include the criminal act, but also the processes that lead up to this act and which form the intention of computer abuse. Analysis of this cognitive process could lead to improved organizational actions that can be taken to avert such violations by extending the zone of control. The purpose of this research commentary has been to address this oversight and provide a clear agenda for future research. Specifically, we have framed our arguments through an extension of the
Straub and Welke (1998) Security Action Cycle. We do not claim that our application of theory for understanding offender behavior is exhaustive, but rather view it as a basis for future studies.

We further contend that this research commentary is timely. In many respects it could be argued that the IS security discipline can be considered the ‘ugly duckling’ of the IS community. Although other IS disciplines have matured, this has not been the case for our field. Such was the conclusion of a paper by Siponen et al. (2008) who pointed to a lack of growth in terms of the levels of empirical research, a paucity of theory and an over emphasis on technical as opposed to more social topics. With this in mind, we believe this research commentary can assist in the maturing of our discipline along these three dimensions.
References


## Appendix A: Neutralization and Moral Disengagement

### Sykes and Matza’s (1957) Techniques of Neutralization

<table>
<thead>
<tr>
<th>Name of technique</th>
<th>Description of technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of responsibility</td>
<td>‘In so far as the delinquent can define himself as lacking responsibility for his deviant actions, the disapproval of self or others is sharply reduced in effectiveness as a restraining influence … delinquent acts are due to forces outside of the individual and beyond his control such as unloving parents, bad companions or slum neighbourhood’. (1957: 667)</td>
</tr>
<tr>
<td>Denial of injury</td>
<td>‘For the delinquent … wrongfulness may turn on the question of whether or not anyone has clearly been hurt by his deviance, and this matter is open to a variety of interpretations. Vandalism may be defined by the delinquent simply as “mischief” … the delinquent frequently and in a hazy fashion, feels that his behaviour does not really cause any great harm, despite the fact that it runs counter to law’. (1957: 667-668)</td>
</tr>
<tr>
<td>Denial of the victim</td>
<td>‘Even if the delinquent accepts the responsibility for his deviant actions and is willing to admit that his deviant actions involve injury or hurt, the moral indignations of self and others may be neutralized by an insistence that the injury is not wrong in the light of the circumstances. The injury, it may be claimed, is not really an injury; rather, it is a form of rightful retaliation or punishment. In addition, however, the existence of the victim may be denied for the delinquent, in a somewhat different sense, by the circumstances of the delinquent act itself. Insofar as the victim is physically absent, unknown, or a vague abstraction (as is often the case against property crimes), the awareness of the victim’s existence is weakened’. (1957: 668)</td>
</tr>
<tr>
<td>Condemnation of the condemners</td>
<td>‘The deviant shifts the focus of attention from his own deviant actions acts to the motives and behavior of those who disapprove of his violations. His condemners, he may claim. Are hypocrites, deviants in disguise, or impelled by personal spite. This orientation toward the conforming world may be of particular importance when it hardens into a bitter cynicism directed against those assigned the task of enforcing or expressing the norms of the dominant society. Police, it may be said, are corrupt, stupid, and brutal. Teachers always show favouritism …The validity of this viewpoint is not so important as its function in turning back or deflecting the negative sanctions attached to violations of the norms. The delinquent, in effect, has changed’</td>
</tr>
</tbody>
</table>
the subject of the conversation in the dialogue between his own deviant impulses and the reactions of others; and by attacking others, the wrongfulness of his own behaviour is more easily repressed or lost to view’. (1957: 668)

<table>
<thead>
<tr>
<th>Appeal to higher loyalties</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Fifth, and last, internal and external social controls may be neutralized by sacrificing the demands of the larger society for the demands of the smaller social groups to which the delinquent belongs such as the sibling pair, the gang, or the friendship clique. It is important to note that the delinquent does not necessarily repudiate the imperatives of the dominant normative system, despite his failure to follow them. Rather the delinquent may see himself caught up in a dilemma that must be resolved, unfortunately, at the cost of violating the law … the most important point is that deviation from certain norms may occur not because the norms are rejected but because other norms, held to be more pressing or involving a higher loyalty, are accorded precedence. It is the fact that both sets of norms are believed in that gives meaning to our concepts of dilemma and role conflict’. (1957: 669)</td>
</tr>
</tbody>
</table>
### Bandura’s (2002) Mechanisms of Moral Disengagement

<table>
<thead>
<tr>
<th>Name of mechanism</th>
<th>Description of mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moral justification</td>
<td>‘People do not usually engage in harmful conduct until they have justified, to themselves, the morality of their actions. In this process of moral justification, pernicious conduct is made personally and socially acceptable by portraying it as serving socially or moral purposes. People then can act on a moral imperative and preserve their view of themselves as moral agents while inflicting harm on others’. (2002: 103).</td>
</tr>
<tr>
<td>Euphemistic labelling</td>
<td>‘Language shapes thought patterns on which actions are based. Activities can take on different appearances depending on what they are called. Euphemistic language is used widely to make harmful conduct respectable and to reduce personal responsibility for it. Euphemising is an injurious weapon. People behave much more cruelly when assaultive actions are given a sanitised label than when they are called aggression’. (2002: 104)</td>
</tr>
<tr>
<td>Advantageous comparison</td>
<td>‘How behaviour is viewed is coloured by what it is compared against. By exploiting the contrast principle reprehensible acts can be made righteous. The more flagrant the contrasting inhumanities, the more likely it is that one’s own destructive conduct will appear benevolent’. (2002: 105).</td>
</tr>
<tr>
<td>Displacement of responsibility</td>
<td>‘Moral conduct operate most strongly when people acknowledge that they are contributors to harmful outcomes … People will behave in ways they normally repudiate if a legitimate authority accepts responsibility for the effects of their conduct. Under displaced responsibility, they view their actions as stemming from the dictates of authorities rather than being personally responsible for them. Because they are not the actual agent of their actions, they are spared self-condemning reactions’. (2002: 106)</td>
</tr>
<tr>
<td>Diffusion of responsibility</td>
<td>‘The exercise of moral control is also weakened when personal agency is obscured by diffusing responsibility for detrimental behaviour … Responsibility can be diffused by division of labour. Subdivided tasks seem harmless in</td>
</tr>
<tr>
<td>Disregard or distortion of consequences</td>
<td>‘Other ways of weakening moral control operate by minimising, disregarding or distorting the effects of one’s action. When people pursue activities that harm others, they avoid facing the harm they cause or minimise it. If minimisation does not work, the evidence of harm can be discredited. As long of the harmful results of one’s conduct are ignored, minimised, distorted, or disbelieved there is little reason for self-censure to be activated … It is easier to harm others when their suffering is not visible and when destructive actions are physically and temporally remote form their injurious effects’. (2002:108)</td>
</tr>
<tr>
<td>Dehumanisation</td>
<td>The strength of moral self-censure depends on how the perpetrators regard the people they mistreat. To perceive another as human activates empathetic reactions through perceived similarity … It is difficult to mistreat humanised people without risking personal distress and self-condemnation … Self-censure for cruel conduct can be disengaged or blunted by stripping people of human qualities. Once dehumanised, they are no longer viewed as persons with feelings, hopes and concerns, but as sub-human objects’. (2002: 109)</td>
</tr>
<tr>
<td>Attribution of blame</td>
<td>‘Blaming one’s adversaries or circumstances is another expedient that serves self-exonerating purposes. People view themselves as faultless victims driven to injurious conduct by forcible provocation. Violent conduct becomes justifiable defensive reaction to belligerent provocations. Victims get blamed for bringing suffering on themselves. Self-exoneration is also achievable by viewing one’s harmful conduct as forced by compelling circumstances rather than as a personal decision. By fixing the blame on others or on compelling circumstances one’s own injurious actions are excusable but one can even feel self-righteous in the process’. (2002: 110).</td>
</tr>
</tbody>
</table>