Recent academic investigations of computer security policy violations have largely focused on non-malicious noncompliance due to poor training, low employee motivation, weak affective commitment, or individual oversight. Established theoretical foundations applied to this domain have related to protection motivation, deterrence, planned behavior, self-efficacy, individual adoption factors, organizational commitment, and other individual cognitive factors. But another class of violation demands greater research emphasis: the intentional commission of computer security policy violation, or insider computer abuse. Whether motivated by greed, disgruntlement, or other psychological processes, 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 of intention (to commit computer abuse) and deterrence (of the crime), but also phenomena which temporally precede these areas. Specifically, we assert the need to consider the thought processes of the potential offender and how these are influenced by the organizational context, prior to deterrence. We believe the interplay between thought processes and this context may significantly impact the efficacy of IS security controls, specifically deterrence safeguards. Through this focus, we extend the Straub and Welke (1998) security action cycle framework and propose three areas worthy of empirical investigation—techniques of neutralization (rationalization), expressive/instrumental criminal motivations, and disgruntlement as a result of perceptions of organizational injustice—and propose questions for future research in these areas.

Keywords: Computer abuse, employee computer crime, information systems security, deterrence, neutralization, motivation, disgruntlement, organizational justice, instrumental crimes, expressive crimes, insider
seek to show that the insider threat is significant and growing, that past IS research about security provided a solid foundation for understanding security in previous times, but also that there are new opportunities to explore this problem in the future.

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 (Mahmood et al. 2008; Hu et al. 2011; Stanton et al. 2005; Warkentin and Willison 2009). Insiders are employees or others who have (1) access privileges and (2) intimate knowledge of internal organizational processes that may allow them to exploit weaknesses. These internal human threats fall along a continuum as indicated in Figure 1, and this range of behaviors is also articulated by Hu et al. (2011) and Guo et al. (2011). Employee violations of security policies may be entirely passive and non-volitional, such as accidental entry of incorrect data values which can threaten data integrity, or can be the actions of employees who are simply careless, sloppy, unmotivated, or poorly trained. (For more discussion of these behaviors, see Stanton et al. 2005.) Other actions by employees might include volitional behaviors that are not motivated by malicious intentions. Guo et al. identify four characteristics of non-malicious security violation: intentional behaviors, self-benefitting without malicious intent, voluntary rule-breaking, and possibly causing damage or security risk. For example, individuals who delay making data backups, fail to shred sensitive documents, fail to encrypt data before transmitting it, fail to change passwords regularly, fail to close a door before discussing sensitive information with a patient in private, or fail to select strong passwords may knowingly be violating security policies, but not with the intent of conflicting specific harm on the enterprise or its information resources. These benign non-malicious insiders may even violate IS security policies with benevolent intentions, such as sharing a password with a coworker who has forgotten his, and the result may occasionally be negative.

At the other end of this continuum is malicious computer abuse by insiders. Intentional malicious noncompliance or abuse can be manifested as data manipulation or destruction, data theft, fraud, blackmail, or embezzlement. Insiders may also steal credit card numbers, may sell intellectual property (such as trade secrets or technologies) to competitors, or may disclose sensitive, classified, or protected information to the public or to enemies of the state. The initial threat from accidents or oversights by careless or unmotivated employees, although it can be the precursor to more extreme incidents, is typically dwarfed by the threat from malicious insider computer abuse by individuals who are motivated to inflict great harm. These insiders are the focus of the present commentary.

While attempts to gain accurate statistics on employee computer abuse are seriously hamstrung by organizational under-reporting due to fears of reputation damage, industry reports and security surveys provide some indication of the problem (CSO Magazine 2007; Ernst & Young 2009; Ponemon Institute 2010; Smith 2009). A recent survey administered to 443 information security and information technology professionals indicated that “twenty-five percent of respondents felt that over 60 percent of their organizations’ financial losses were due to non-malicious actions by insiders” (Richardson 2009). Forty-three percent of respondents stated that “at least some of their losses were attributable to malicious insiders” (Richardson 2009). Furthermore, the UK National Hi-Tech Crime Unit (NOP World 2005) reported that 38 percent of financial fraud, 68 percent of theft of information or data, and 100 percent 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 organizations that experienced breaches, just under half were committed inside the company. A survey by PwC (PwC/DoBERR 2008) found that for large organizations (250+ employees), 57 percent of the respondents reported the cause of their worst security incident to be internal, and the Global State of Information Security survey (PwC 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 number 1 and number 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” (Carr 2007). In 2011, Symantec reported that the cost of Intellectual Property theft (such as data breaches) to U.S. businesses was more than $250 billion/year, that these thefts should double within the next decade, and that “the most frequent perpetrators were current or former employees” (Shaw and Stock 2011, p. 4).

A breach by even one malicious employee can be potentially devastating (Warkentin and Willison 2009; Willison and Siponen 2009). In addition to insider access, workplace training and exposure gives employees the skills, knowledge, and resources that provide them with the means to implement successful computer abuse (Parker 1998). Knowledge of security loopholes can be exploited by rogue employees via access to computing resources that is provided by the organization. Further, motivation to commit criminal violations may be created as a result of workplace disgruntlement. A malicious employee can, therefore, use these attributes for the commission of computer abuse, which, in the extreme, can bring down an organization. Support for this argument comes from Workentin (1995) and others, identifying a calculus of risk-based cost for evaluating each specific threat to informa-
The IS security community has responded to these concerns about insider abuse by undertaking a large number of studies that have examined the issue of compliance or noncompliance with policies. These studies have largely focused on the behavior of well-intentioned employees and examined factors which either hinder or facilitate compliance with security policies (Boss et al. 2009; Bulgurcu et al. 2010; Dodge et al. 2007; Herath and Rao 2009; Johnston and Warkentin 2010; Lee and Larsen 2009; Myyry et al. 2009, Pahnila et al. 2007; Sasse et al. 2001; Siponen and Vance 2010; Straub 1990; Workman et al. 2008). In Figure 1, these violations generally fit with the volitional, but non-malicious, actions of employees. Such violations, although significant, are often dwarfed by a major insider abuse event in terms of their cost to the enterprise. Admittedly, there exists research which has focussed on the insider threat in terms of their motivation (Shropshire 2009; Straub 1990), deterrence (D’Arcy et al. 2009; Harrington 1996; Hoffer and Straub 1989; Straub 1990; Straub et al. 1992; Straub and Welke 1998), intention to offend (Foltz 2000; Lee and Lee 2002; Lee et al. 2004; Workman and Gathegi 2007), and prevention (Willison 2002, 2006; Willison and Backhouse 2006; Willison and Siponen 2009). However, this body of work is relatively modest when compared with the compliance literature, and warrants further consideration (Mahmood et al. 2010; Warkentin and Willison 2009).

To aid our discussion of the insider threat, we discuss and extend 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 abuse, followed by efforts targeted at detection, and finally the pursuit of remedies.

---

2Siponen et al. (2008) concluded that the IS security field has not matured as other IS disciplines have, pointing to a lack of growth in terms of the levels of empirical research, a paucity of theory, and an overemphasis on technical as opposed to more social and behavioral topics. Subsequent work has begun to introduce more theoretically justified work.
Importantly, Straub and Welke argued that organizations must attempt to maximize deterrence and prevention efforts, while minimizing the need for detection and remedy. We argue that a more holistic focus must extend beyond the security action cycle by encompassing phenomena which temporally occurs prior to deterrence (Willison and Warkentin 2010). Specifically, we assert the need to consider the thought processes of the potential offender and the organizational context. This consideration is advocated because we believe the interplay between thought processes and this context may significantly impact the efficacy of IS security controls, specifically deterrence safeguards.

The rest of the paper is structured as follows: In the next section, we propose and develop the general extension to the Straub–Welke security action cycle, which we call the extended security action cycle. This framework is grounded in a discussion of the existing literature, to help contextualize our argument and illustrate how rarely the IS security field has examined phenomena which may temporally occur prior to deterrence. Based on this observation, we then propose three new areas for future IS security research—neutralization techniques, expressive/instrumental criminal motivations, and disgruntlement as a result of perceptions of organizational injustice—and offer research questions for the consideration of security scholars. It should be noted that these areas are designed to be illustrative, rather than exhaustive, and that other phenomena, which occur prior to deterrence, may also prove influential. Finally, we conclude by discussing the potential for combining the three, plus other, areas for future research, and discuss the possible benefits in studying IS security phenomena from a more holistic and longitudinal perspective.

Computer Abuse Timeline

To aid our discussion of employee computer crime, we introduce Figure 3, which contextualizes our argument by illustrating the events which occur prior to deterrence and focus on the “pre-kinetic” events. The feedback loops in the

---

3The concept of looking at pre-kinetic events is inspired by so-called fourth-generation military strategy, which has identified the need to focus on the temporal antecedents of military aggression, or “left of bang,” in an effort to gain a richer understanding of the causes of such actions (Allen 2009) so they can be avoided in the future.
original action cycle and the category “remedies” are still presumed to be operational, and have been omitted from Figure 3 for the sake of clarity.

Along the timeline in Figure 3, T₀ depicts the key moment in which the offender has successfully managed to perpetrate some form of computer abuse. Working backward along the timeline, and therefore moving to the left, is the category called “prevention.” Within this category, there is a body of research which focuses on the offender and attempts to examine offender behavior in the organizational context (Willison 2002, 2006; Willison and Backhouse 2006; Willison and Siponen 2009). To the left of prevention is the point called “behavioral intention.” While intention is not highlighted in the Straub and Welke model, a number of researchers have addressed the concept. Specifically, researchers have combined a number of theories in order to understand those factors which together form behavioral intention (Foltz 2000; Lee and Lee 2002; Lee et al. 2004; Workman and Gathegi 2007). One of these factors is deterrence, which has been the focus for several IS security researchers and represents, by far, the most studied area of employee computer abuse (D’Arcy and Hovav 2007; D’Arcy et al. 2009; Harrington 1996; Hoffer and Straub 1989; Straub 1990; Straub et al. 1992; Straub and Welke 1998). Of some significance, however, is the fact that phenomena which exist temporally prior to deterrence have rarely been addressed by IS security researchers. Indeed, only two papers by Straub (1990) and Shropshire (2009) have considered such phenomena by examining the issue of motive.

We, however, believe that recognition of phenomena which temporally occur prior to deterrence is of key importance. Specifically, we assert the need to consider the relationship between the thought processes of the potential offender and the organizational context. This consideration is advanced as we believe the interplay between the two may significantly impact the efficacy of IS security controls, specifically deterrence safeguards. We elaborate on these arguments in the following three sections of the paper.

Research Area 1: Criminal Justifications and Deterrence

The first area focuses on how individuals may attempt to rationalize or justify their criminal behavior and how this
Research with comparable themes and findings was published by the eminent psychologist Albert Bandura (1986, 1999, 2002; Bandura et al. 1996). Instead of techniques of neutralization, Bandura argued that individuals use mechanisms of moral disengagement in an attempt to justify their deviant/criminal behavior.

What We Know: Techniques of Neutralization

In their seminal text, Sykes and Matza (1957) rejected the idea of a delinquent subculture in which the prevailing values represent an inversion of those held by respectable society. They argued that delinquents show signs of commitment to the dominant social order by exhibiting feelings of guilt and shame when laws are broken. Furthermore, young offenders often respect and admire figures who conform to the social order (e.g., a law abiding mother). Finally, Sykes and Matza observed that delinquents often discriminate between what are perceived by them to be “appropriate” and “inappropriate” targets. This last point is illustrated by the authors with the maxims “don’t commit vandalism against a church of your own faith” and “don’t steal from friends,” indicating how some elements of the social order are deemed sovereign by delinquents.

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” or 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, which are cited in Table 1, along with other techniques discussed below. 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).

Subsequent researchers have identified other techniques of neutralization used by criminal offenders to justify their actions, which are also presented in Table 1.

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 (for an extensive review, see Maruna and Copes 2005). This range of criminal behaviors is summarized in Table 2.

Advocating the application of the techniques of neutralization for the organizational context may appear strange, particularly given that it was first advanced as a theory of delinquency. However, existing research would appear to suggest otherwise (Ingram and Hinduja 2008; Maruna and Copes 2005). Hollinger (1991), for example, researched four techniques of neutralization with regard to self-reported property and production deviance. His study found that the highest levels of these forms of deviance were reported by those employees who evoked the denial of the victim and denial of injury. In a later study of corporate crime, Piquero et al. (2005) found that the appeal to higher loyalties and denial of injury were significant predictors with regard to the intention to engage in this form of behavior. Another related point is that techniques of neutralization may be particularly worthy of study in the corporate context, as employees have a far greater stake in conventional society, and may be less committed to their criminal behavior, than hardened offenders (Copes and Williams 2007; Ingram and Hinduja 2008; Paternoster and Simpson 1996). This would suggest that corporate employees are far more open to feelings of guilt and shame, as opposed to career criminals. Indeed, such findings have led Maruna and Copes to note that “neutralization theory has found its most receptive audience in studies of organization and white-collar crime” (p. 223).
Table 1. Techniques of Neutralization

<table>
<thead>
<tr>
<th>Technique</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of responsibility</td>
<td>Sykes and Matza (1957)</td>
</tr>
<tr>
<td>Denial of injury</td>
<td>Sykes and Matza (1957)</td>
</tr>
<tr>
<td>Denial of the victim</td>
<td>Sykes and Matza (1957)</td>
</tr>
<tr>
<td>Condemnation of the condemners</td>
<td>Sykes and Matza (1957)</td>
</tr>
<tr>
<td>Appeal to higher loyalties</td>
<td>Sykes and Matza (1957)</td>
</tr>
<tr>
<td>Metaphor of the ledger</td>
<td>Klockars (1974)</td>
</tr>
<tr>
<td>Defense of the necessity</td>
<td>Minor (1981)</td>
</tr>
<tr>
<td>Avoidance of greater harm</td>
<td>Garrett et al. (1989)</td>
</tr>
<tr>
<td>Legal rights</td>
<td>Garrett et al. (1989)</td>
</tr>
<tr>
<td>Comparative standards</td>
<td>Garrett et al. (1989)</td>
</tr>
<tr>
<td>Malicious intentions</td>
<td>Garrett et al. (1989)</td>
</tr>
<tr>
<td>Defense of the necessity of the law</td>
<td>Coleman (1994)</td>
</tr>
<tr>
<td>Claim of entitlement</td>
<td>Coleman (1994)</td>
</tr>
<tr>
<td>Claim of relative acceptability</td>
<td>Henry and Eaton (1994)</td>
</tr>
<tr>
<td>Claim of individuality</td>
<td>Henry and Eaton (1994)</td>
</tr>
<tr>
<td>Postponement</td>
<td>Cromwell and Thurman (2003)</td>
</tr>
<tr>
<td>Justification by comparison</td>
<td>Cromwell and Thurman (2003)</td>
</tr>
</tbody>
</table>

Table 2. Criminal Behaviors Employing the Techniques of Neutralization

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drug abuse</td>
<td>Priest and McGrath (1970)</td>
</tr>
<tr>
<td>Tax evasion</td>
<td>Thurman (1984)</td>
</tr>
<tr>
<td>White-collar crime</td>
<td>Benson (1985)</td>
</tr>
<tr>
<td>Domestic violence</td>
<td>Dutton (1986)</td>
</tr>
<tr>
<td>Poaching</td>
<td>Eliason and Dodder (1999)</td>
</tr>
<tr>
<td>Car theft</td>
<td>Copes (2003)</td>
</tr>
<tr>
<td>Shoplifting</td>
<td>Cromwell and Thurman (2003)</td>
</tr>
<tr>
<td>Corporate crime</td>
<td>Piquero et al. (2005)</td>
</tr>
</tbody>
</table>

What We Know: IS Research and Rationalizations

As discussed, the techniques of neutralization have been applied to research diverse forms of deviant or criminal behavior. Given this, it is perhaps no surprise to learn that these forms of behavior have recently encompassed IS related areas. One such area has been the study of “cyberloafing” in the organizational context (Lim 2002; Lim and Teo 2005). This form of deviance occurs when an employee uses their company’s Internet resources for personal use. In an attempt to explain this behavior, Lim (2002) applied the “metaphor of the ledger” (Klockars 1974). With this technique of neutralization, an individual compares their levels of deviance with their nondeviant levels of behavior. By so doing, an individual is able to rationalize the former as relatively minor and justified, when compared with their overall honest actions. Lim found significant and positive support for this
technique of neutralization, as a means for explaining cyberloafering. Other studies have addressed neutralization processes used in digital piracy (Hinduja 2007; Ingram and Hinduja 2008, Morris and Higgins 2009). Ingram and Hinduja (2008) applied the five original neutralization techniques for researching the illegal downloading of MP3 files. Based on 2,032 responses from undergraduate students in a large U.S. university, four of the techniques (excluding “condemnation of the condemners”) were found to be significant predictors of moderate (101–1000 downloads in the prior year) piracy. Finally, Siponen and Vance (2010) studied the rationalization process with regard to non-compliance with information security policies. The original five neutralization techniques advanced by Sykes and Matza, plus the “defense of necessity” (Minor 1981) and the “metaphor of the ledger” (Klockars 1974) were applied. The study found “that neutralization is an excellent predictor of employees’ intention to violate IS security policies” (Siponen and Vance 2010, p. 10).

While Siponen and Vance’s study acts as a contribution to the compliance literature, earlier IS security work has considered how dishonest employees may rationalize computer abuse (Harrington 1996; Willison 2002, 2006). As noted, Harrington (1996) examined the influence of denial of responsibility and its moderating influence on computer abuse judgments and intentions. At a conceptual level, Willison (2002, 2006) suggested the application of neutralization techniques for greater insights into the perpetration of employee computer abuse. Of particular relevance for IS security is the relationship between techniques of neutralization and deterrence in the organizational context. As noted, these neutralizations are employed by individuals to mitigate feelings of guilt and shame associated with a deviant act. Interestingly, the criminological literature has noted that shame acts as a deterrent in a similar fashion to formal or informal sanctions (Braithwaite 1989; Nagin and Paternoster 1993; Paternoster and Simpson 1996; Piquero and Tibbetts 1996). Indeed, a number of studies have applied shame as a separate deterrence construct (Nagin and Paternoster 1993; Paternoster and Simpson 1996; Piquero and Tibbetts 1996). Two more recent studies in the IS security field have also applied shame in this manner (Hu et al. 2011; Siponen and Vance 2010). The aforementioned criminological literature also illustrates how employees may be particularly susceptible to feelings of guilt and shame, given their stake in conventional society and only partial commitment to criminal behavior. This may, therefore, explain why techniques of neutralization have been found to be most influential in the organizational context, as individuals in such a context are more likely to invoke them.

What We Need to Learn: Future Research Questions

Given this theoretical foundation, the study of neutralization techniques would appear to offer some promise regarding our understanding of the insider threat. With the relative lack of empirical research in this area, initial studies may wish to consider the techniques in relation to specific forms of computer abuse, which type of person evokes them, which technique is selected in which circumstance, and their influence on the effectiveness of deterrence. Research addressing these areas would not only broaden our understanding of employee computer abuse, but also provide a firm basis for contemplating intervention strategies.

Research Question 1a: Which rationalizations are associated with specific forms of employee computer abuse? Although Sykes and Matza 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). A useful starting point, therefore, would be to identify which rationalizations, if any, are associated with particular forms of employee computer abuse.

Research Question 1b: Do techniques of neutralization predict employee’s intention to commit computer abuse? This section has highlighted how an individual can invoke techniques of neutralization to mitigate feelings of guilt and shame. In addition, organizational members, compared with hardened criminals, may have a considerable stake in society and only a partial commitment to criminal behavior. Researchers have noted, therefore, that employees are more likely to draw on techniques of neutralization in an attempt to avoid the feelings of guilt and shame (Copes and Williams 2007; Maruna and Copes 2005). As these feelings have been noted to yield a deterrent effect (Nagin and Paternoster 1993; Paternoster and Simpson 1996), their absence may leave an individual free to offend. This could well explain why techniques of neutralization have been found to exert a considerable influence on deviant acts in the organizational context, and may also help to explain employee computer abuse.

Research Question 1c: Is there a curvilinear relationship between techniques of neutralization and computer abuse? Recent research has indicated that the relationship between rationalizations and deviance is curvilinear (Copes and Williams 2007; Ingram and Hinduja 2008; Maruna and Copes 2005). 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 digital 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.

**Research Area 2: Expressive and Instrumental Motives and Deterrence**

Our next proposed research area 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 abuse, 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 (Burek 2006; Ekblom 1997) 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 of acquiring cash. Expressive crimes often involve frustration, anger, rage, and despair. Unlike instrumental offenses, the actual commission is considered an end in itself (Burek 2006; Ekblom 1997) and there is no additional goal to be met. Cases of aggravated assault, for example, may involve the resolution of anger issues.

The instrumental/expressive distinction has been used by criminologists to address a diverse range of crimes including terrorism (Amir 1988), rape (Rosenberg et al. 1988), vandalism (Whittingham 1981), workplace violence (Swanton 1989), intra-family violence (Dawson 2006; Gelles 1987), arson (Fritzon 2001; Hakkonen 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 offense can be categorized along instrumental or expressive lines (Block and Christakos 1995; Polk 1994).

**What We Know: Deterrence and Expressive Motivations**

For this paper, the greatest significance of the distinction between expressive and instrumental motives concerns the implications for deterrence. Specifically, authors within the field of criminology have argued that deterrent sanctions apply most readily to crimes with instrumental motives, whereas offenses driven by expressive ones are considered harder to deter (Chambliss 1967; Parker and Smith 1979; Thomas and Williams 1977; Zimring and Hawkins 1973). Chambliss (1967), for example, argued that the efficiency of deterrence is dependent on two factors. The first factor is whether the crime is instrumental or expressive in nature, and the second is whether an individual has a low or high commitment to crime. Combining these two distinctions, he 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 who undertake expressive criminal acts are least likely to be deterred.

Whatever the merits of the arguments advanced by Chambliss and others, Nagin (1998) noted how the deterrence literature has not resolved the issue of whether expressive-based crimes are less deterrable than instrumental offences. However, more recent work in criminology, and specifically deterrence, has made inroads into this problem, and has opened up new avenues of research for consideration in the IS security field.

As noted earlier, expressive crimes often involve the offender experiencing emotions such as rage, anger, and despair. Given this, of particular relevance to the current text are a number of deterrence studies (Ariely and Lowenstein 2006; Bouffard 2002; Bouffard et al. 2000; Carmichael and Piquero 2004; Exum 2000; Lowenstein et al. 1997), which took their inspiration from a body of work examining the more general relationship between emotions and behavior (Dunegan et al. 1992; Lerner and Keltner 2000; Lowenstein 1996). Lowenstein (1996), for example, argued that emotions directly affect all forms of behavior and that the level of influence is proportionate to the level of emotions. Hence, an individual experiencing very strong emotions, a state which Lowenstein terms “out of control,” will behave contrary to their own self-interest. Supporting studies further noted the influence of emotions on cognitive tasks such as making judgments and decisions (Dunegan et al. 1992; Lerner and Keltner 2000).
With this in mind, a number of criminologists began to examine the extent to which emotions may influence the perceived threat of sanctions when criminal decisions are made. Boufard et al. (2000) noted how an individual’s emotional state acts as an important foundation for rational decision making. When an individual experiences emotional intensity, his or her ability to rationally deliberate and accurately assess the perceived costs and benefits associated with a crime is impinged. Strong emotions focus the attention of an individual on the present, where the benefits of crime are obvious and potentially gratifying, at the expense of considering the costs associated with the criminal act. If a crime ensues, the skewed assessment of costs and benefits, taking place in a narrowed time horizon, helps to explain why an individual’s behavior can appear contrary to their own self-interest (Lowenstein 1996).

Other studies have empirically examined such behavior. Carmichael and Piquero (2004), for example, examined the inter-relationships between emotional arousal, perceived sanction threats, and criminal intention. As a starting point, the researchers drew on the work of Zimring and Hawkins (1973), who hypothesized that emotional arousal, neither formal nor informal sanctions may influence deterrence efficacy. Several writers have noted how the influence of emotions is proportionate to their level of intensity, his or her ability to rationally deliberate and accurately assess the perceived costs and benefits associated with a crime is impinged. Strong emotions focus the attention of an individual on the present, where the benefits of crime are obvious and potentially gratifying, at the expense of considering the costs associated with the criminal act. If a crime ensues, the skewed assessment of costs and benefits, taking place in a narrowed time horizon, helps to explain why an individual’s behavior can appear contrary to their own self-interest (Lowenstein 1996).

The context in which decisions to commit or refrain from crime are made will presumably have some bearing on the relative influence of threats in the decisional process. Decisions that are made very quickly, as a reaction to a sudden impulse, may be less susceptible to the influence of threats than decisions that are arrived at over longer periods. Decisions about criminal conduct that are made when a person is in circumstances which provoke great emotional arousal may be less amenable to threats than decisions that occur when the potential criminal is less aroused, because very high degrees of emotional arousal may eclipse thoughts of future consequences by riveting all of the potential criminals attention on his present situation (pp. 136-137).

In their research, therefore, Carmichael and Piquero combined the role of emotion, specifically anger, in a deterrence/rational choice model. To examine this relationship, respondents were first asked to read a scenario and then answer questions relating to their perceptions and proposed actions. It was hypothesized that individuals under high perceived emotional arousal would be more influenced by perceived benefits than perceived costs, while those experiencing low to moderate anger perceptions would be influenced more by the perceived costs rather than the perceived rewards. Carmichael and Piquero’s results supported these hypotheses. For those who perceived low to moderate anger, informal sanctions did relate to assault intention. However, for those who perceived high emotional arousal, neither formal nor informal sanctions inhibited criminal intention.

**What We Need to Learn: Future Research Questions**

Examining the relationship between emotions and deterrence would represent a new stream of research for the IS security field. Such a focus would prove useful for assessing the efficacy of IS security deterrent safeguards, and the associated sanction threats, when addressing forms of computer abuse underpinned by strong emotions. Hence, a more sophisticated understanding of the situations where deterrent controls are, and are not, effective may be afforded when emotions are considered. Indeed, some writers have even gone so far as to argue that theories of decision making which omit the role of emotion may be incomplete (Carmichael and Piquero 2004; Frazier and Meisenhelder 1985). Such may be the case with regard to general deterrence theory, which has proved a staple theory for the IS security discipline.

**Research Question 2a:** Do emotions moderate the threat of sanctions created by IS security deterrent safeguards? While it has been noted that criminological deterrence research based on the rational choice assumption has all but overlooked the influence of emotions in offender decision making (Bouffard et al. 2000; Carmichael and Piquero 2004), this is certainly the case with regard to the IS security discipline. Examining the relationship between deterrence and emotions is timely, as the aforementioned studies appear to cast doubt on the efficacy of the former, in some circumstances, when influenced by the latter. As noted earlier, not all crimes are committed by fully rational offenders, which is also the case when considering the diverse forms of computer abuse. Some instances of computer sabotage may well represent examples of abuse where emotions exert a considerable influence. A good starting point would be to consider if emotions moderate the threat of sanctions created by IS security deterrence controls.

**Research Question 2b:** Do different levels of emotions moderate or mediate the threat of sanctions created by IS security deterrent safeguards? Closely related to the above question is consideration of how differing levels of emotion may influence deterrence efficacy. Several writers have noted how the influence of emotions is proportionate to their level (Bouffard et al. 2000; Lowenstein 1996). Hence, it is suggested that at high levels of emotion, consideration of future
costs is impinged as the offender’s attention is focused on the present situation, as confirmed by Carmichael and Piquero.

Research Question 2c: To what extent do personality traits influence the relationship between emotions and deterrence? Interestingly, in the Carmichael and Piquero paper, the authors note how anger can either take the “trait” or “state” forms. The former relates to a personality trait or disposition, while the latter is a state or situational emotion, which can fluctuate and vary in intensity over time. One potential area for future research, therefore, would be to consider the influence of personality traits on the relationship between emotions and deterrence. These traits would be expected to either positively or negatively moderate the influence of emotions on deterrence efficacy. Deterrence research in the field of criminology has already started to examine the influence of personality traits (e.g., Piquero and Tibbets 1996; Wright et al. 2004), and noting their influence in combination with situational factors would appear a logical extension for the IS security discipline.

Research Area 3: Injustice and Disgruntlement as Motives

The third area to consider focuses on the issue of motives for employee computer crime. This currently represents an under-researched subject for the IS security field, but we argue that progress may be achieved by considering motives in relation to workplace disgruntlement. A report by the U.S. Secret Service and Carnegie-Mellon University (Keeney et. al. 2005), entitled “Insider Threat Study: Computer Systems Sabotage in Critical Infrastructures,” studied 49 cases of insider sabotage. One of the key findings was that in 83 percent of cases, the perpetrator held a “work-related grievance” and that grievances of this type act as a trigger for criminal actions.

What We Know: 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 that relate to different organizational phenomena and influence employees’ perceptions of fairness/unfairness in organizations or what is interchangeably termed justice/injustice. What has emerged is a voluminous amount of research which has focused on these constructs (entitled distributive, procedural, interactional, and informational justice), and the theories that underpin them (Cohen-Charash and Spector 2001; Colquitt et al. 2001). Of specific importance are the implications of motives for IS security. While we acknowledge that disgruntlement factors are generic to the organizational domain (i.e., not IS-specific), we argue that consideration of this problem is still worthy of examination through organizational justice constructs, as it may provide critical insights into the form of, and the goals behind, insider computer abuse. In addition, we further claim that the source of perceived injustice may provide a far greater understanding of the target for abuse than currently exists. Therefore, while the factors creating motives are generic to the organizational domain, the impacts of these motives have significant implications for IS security. Before we elaborate on this argument, we will briefly describe the four types of organizational justice.

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 termed “normative expectations,” which are learned through socialization in forums such as the home, school, and work. Crucially, Adams (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

Leventhal and his colleagues (Leventhal 1980; Leventhal et al. 1980) were the first to address procedural justice in the organizational context by focusing on the nature of the procedures and the implications for 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 Justice

Based on seminal research by Bies and Moag (1986), Greenberg (1990, 1993) proposed two further organizational justice constructs entitled interpersonal and informational justice. Interpersonal justice refers to the manner of treatment by those in authority over their subordinates. This form of justice, therefore, is fostered when supervisors treat their staff with politeness, dignity, and respect and when they refrain from improper comments or remarks. Greenberg regards this construct as 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.

Informational Justice

Informational justice focuses on those factors related to how decisions are explained by senior members of staff to their juniors (Greenberg 1990, 1993). Hence, the extent to which explanations are considered honest and thorough formed the basis of this construct. In addition, Greenberg noted how this form of justice is closely related to its procedural form. The 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 subsequent study, Shapiro et al. (1994) added to the informational justice literature through their research into factors that 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, timely, and specific (i.e., tailored to the individual).

What We Know: Organizational Justice and Workplace Deviance

A number of studies have also addressed the reactions that impact organizations as a consequence of perceptions of justice/injustice (for an extensive review of this literature, see Cohen-Charash and Spector 2001; Colquitt et al. 2001; Nowakowski and Conlon 2005). 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 and Tripp 1998; Bies et al. 1997), workplace violence (Greenberg and Barling 1999), and sabotage (Giacolone et al. 1997). Yet it has been argued that the above studies are relatively “coarse-grained” and have ventured only to look at the relationship between the effect of injustice (be it distributive, procedural, interactional, or informational in nature) and whether or not a staff member engages in a specific deviant act, such as theft (Ambrose et al. 2002). In addition, little attention has been paid to consideration of how the type of injustice may affect the subsequent form of, and goals behind, workplace deviance. It has also been suggested that the source of perceived injustice may provide critical insights into the target of the ensuing deviance (Ambrose et al. 2002; Hirschcovis and Barling 2010; Jones 2009). Consideration of these areas could provide key insights into understanding, predicting, and, ultimately, controlling various forms of deviance (Jones 2009), which could obviously include employee computer abuse.

To address these noted deficiencies, a good starting point is to consider the work of Ambrose et al. (2002), who examined the relationship between organizational justice and sabotage. Previous research which had examined distributive justice and deviance noted that individuals who felt underpaid developed perceptions of injustice. In response, some individuals would steal items of organizational property. Hence, it was concluded that the underlying goal of such theft was equity restoration (Sieh 1987). However, other research has equally noted that individuals who perceive themselves to be unfairly treated by others may engage in acts of revenge against them (Bies and Tripp 1998; Bies et al. 1997). Indeed, this is consistent with previous management studies, which have observed how organizational deviance, in general, can serve expressive or instrumental goals (Dubois 1979; Robinson and Bennett 1997), and also with our own observations raised in Research Area 2. Robinson and Bennett (1997, p. 16) described the former’s goals as to “vent, release or express
one’s feelings of outrage, anger or frustration,” while the latter involves “repairing the situation, restoring equity, or improving the current situation.” Given this, Ambrose et al. hypothesized that those individuals who experience distributive injustice will engage in sabotage which affords equity restoration, while those who experience interpersonal injustice will engage in sabotage as an act of retaliation. This hypothesis was confirmed.

A second area addressed by Ambrose et al. focused on the target of deviance. Prior organizational justice literature had established a distinction between structural and social forms of injustice (Folger and Skarlicki 1998; Greenberg 1993). Structural forms of injustice (distributive and procedural) are recognized as being created by the organization, while their social counterparts (interpersonal and informational) arise from interaction between supervisors and their subordinates. Importantly, studies suggest that the target of deviance corresponds with the perceived source (Robinson and Bennett 1995; Sheppard et al. 1992). In their research, Ambrose et al. tested this observation. They hypothesized that the targets of sabotage behaviors, be they organizational or individual, would match the perceived source of injustice, be they structural (in their study this related solely to distributive injustice) or social (interpersonal and informational). The hypothesis was subsequently confirmed, although the relationship was stronger between the source and organizational targets, when compared with the source and individual ones.

Importantly, more recent research has confirmed the findings of Ambrose et al. A number of studies have illustrated how the type of injustice may predict the form of, and goal behind, organizational deviance (Inness et al. 2005; Jones 2009; Mitchell and Ambrose 2007). Jones (2009) found that perceptions of interpersonal and informational injustice explained more variance of counterproductive workplace behavior directed at a supervisor when compared with perceptions of distributive and procedural injustice. In addition, the study found that procedural justice explained more variance of counterproductive workplace behavior aimed at the organization when compared with distributive, interactional, or informational injustice.

In terms of the target of deviance, several studies mirror the findings of Ambrose et al. (e.g., Hershcovis et al. 2007; Holtz 2009; Inness, et al. 2005; Jones 2003, 2009; Masterson et al. 2000; Mitchell and Ambrose 2007). In a meta-analysis of 57 empirical studies, Hershcovis et al. (2007), for example, found interpersonal treatments by supervisors to be a strong predictor of supervisor-targeted aggression.

**What We Need to Learn: Future Research Questions**

To expand our understanding of the role of perceived organizational injustice in the timeline of cognitive processes preceding computer abuse, the scholarly community must develop a richer, more nuanced knowledge set regarding the impacts of each form of injustice on the mindset of employees, as well as the potential organizational actions in this domain. What will disgruntlement lead to? Will sanctions be effective against this source of motivation?

**Research Question 3a:** Do structural forms of injustice lead to instrumental forms of computer abuse? Do social forms of injustice lead to expressive forms of computer abuse? The relevant literature appears to suggest that distributive and procedural injustice may result in instrumental acts of equity restoration (e.g., computer fraud or embezzlement), while the social forms of injustice, particularly interpersonal, will lead to expressive acts (e.g., sabotaging a database).

**Research Question 3b:** In the organizational context, are the various forms of employee computer abuse, borne out of the different forms of injustice, equally deterrable? Importantly, the relationship between organizational injustice and deterrence has rarely been considered in the management literature (Trevino 1992). Yet, as this section has highlighted, while the factors that create perceptions of injustice are generic to the organizational context, if these perceptions are borne by individuals working with an IS, how effective are the IS deterrent safeguards? As we have illustrated, if the type of injustice plays a significant role in determining the subsequent form of (and goals behind) the ensuing deviance, this may significantly impact the extent to which the ensuing deviance is deterrable. Given the literature in this section and the previous section, is it the case that forms of computer abuse based on perceptions of distributive and procedural injustice are more open to the threat of sanctions when compared with more expressive forms of abuse, based on perceptions of interpersonal and informational injustice?

**Research Question 3c:** Do the forms of injustice predict the target of computer abuse? To date, consideration of the target has received little attention in the IS security field (Willison 2002; Willison and Backhouse 2006). However, as noted, the source of injustice may also act as the subsequent target (Ambrose et al. 2002; Hershcovis and Barling 2010; Jones 2009). Earlier security research (Willison 2006) has indicated that the type of deviance undertaken will be influenced by the choice-structuring properties (i.e., features of criminal activities which make them more attractive or available to specific individuals; Cornish and Clarke 1989). For example,
Conclusion

While numerous studies have focused on the security behavior of employees without regard to the motivational factors (although greater granularity was offered by Guo et al. 2011) or only with regard to non-malicious noncompliance with security policies, little attention has been paid to those staff members who perpetrate deliberate and malicious computer abuse. The purpose of this research commentary has been to address this oversight and provide a research agenda for possible future studies. Past research provided a solid foundation for understanding security violations, but with new and growing threats, especially from inside sources, we call for new perspectives and new theoretical lenses, especially for the malicious insider abuse problem. We argue that our research focus must include not only the criminal act and its immediate antecedents of intention (to commit the abuse) and deterrence (of the crime), but also phenomena which temporally precedes these areas. Specifically, we assert the need to consider the thought processes of the potential offender and how these are influenced by the organizational context prior to deterrence. This consideration is suggested as we believe the interplay between thought processes and this context may significantly impact the efficacy of deterrence safeguards.

We have framed our arguments through an extension of the Straub and Welke (1998) security action cycle, and proposed three areas of specific research focus, each including a series of research questions for future studies. Although the three proposed areas have been discussed in isolation, we would suggest that these, and potentially other topics for consideration, might prove fruitful when studied together. For example, research into organizational justice would also appear to link well with the work on criminal justifications/rationalizations. As noted, for example, distributive justice focuses on perceptions of fairness with regard to decision outcomes. Adams (1965) argued that individuals compare the ratios of their work outputs (rewards) and inputs (contributions) to the ratio of a comparative other (e.g., a work colleague). Therefore, if staff members A and B have the same inputs, but A finds out that B is paid 25% more than he is, perceptions of a lack of distributive justice would occur. A may also feel justified in restoring the balance of equity through committing computer fraud. He may also draw on techniques of neutralization to reinforce his justifications. A may rationalize his or her actions in a manner which leads to denial of the victim. In this case, there is an insistence [by the offender] that the injury is not wrong in light of the circumstance. The injury, it may be claimed, is not really an injury; rather it is a rightful form of rightful retaliation or punishment. Hence, A may claim that “they (the organization) deserve it” because he’s paid less than B despite performing the same job functions (Sykes and Matza, 1957, p. 668).

The three research areas may also be used for studying other subject matter in the IS security field. To illustrate this point, we will briefly consider security policy compliance. When examining this subject, a number of researchers have applied general deterrence theory (D’Arcy et al. 2009; Harrington 1996; Straub 1990). As noted, emotions may impact deterrence efficacy with regard to employee computer abuse. However, could this not also be the case with regard to policy compliance by employees? In a similar vein, a number of management studies have examined how compliance is influenced by perceptions of organizational justice/injustice (Lind and Tyler 1988; Tyler 1990; Tyler and Huo 2002; Wenzel 2006). Wenzel’s (2006) study of Australian tax regulations is a case in point. His research found that tax reminder letters, which embodied principles of interpersonal and informational justice, yielded far greater compliance rates when compared with the standard Australian Taxation Office letters, which explicitly stated sanctions based on deterrence principles. The final area involves consideration of the relationship between compliance and techniques of neutralization. As noted, initial research into this relationship was conducted by Siponen and Vance (2010). This study may be extended by examination of the situations which must occur for the evocation of the neutralization techniques (Agnew 1994; Agnew and Peters 1986; Sykes and Matza 1957). While we have noted the relationship between techniques of neutralization and organizational justice, from an offender’s perspective, the same theoretical relationship may also be applied for examining factors that lead to the adoption of such techniques for rationalizing noncompliant behavior.

A final point worth mentioning concerns the manner in which academic disciplines attempt to identify and demarcate appropriate subject matter, and the implications for researching phenomena. This can, perhaps, be best explained by an example. As noted in Research Area 3, organizational justice studies have not considered the possible influence of sanction threats. This is understandable, given that organizational justice research has largely been undertaken by scholars in the management field and deterrence has been researched by IS.
security academics. On the face of it, a perfectly reasonable argument might then be raised that organizational justice is not IS-specific and should, therefore, not be studied. However, as this text has illustrated, factors which have traditionally been considered outside the remit of IS security clearly have implications for the discipline subject matter. While past research has called for a focus on the IT artifact (Orlikowski and Iacono 2001) in a bid to help focus our discipline, we would suggest that, at times, academic boundaries may hinder knowledge development. We hope to have illustrated that a greater focus on the social artifact (i.e., the offender, in this instance) has opened up new avenues for productive future research within our discipline.

Acknowledgments

We gratefully acknowledge the suggestions, advice, and encouragement from Detmar Straub and other members of the IFIP Working Group 8.11/11.13 (IS Security Research) on earlier versions of this manuscript (Willison and Warkentin 2009, 2010). We also acknowledge the helpful suggestions of Richard Baskerville and the three anonymous reviewers.

References


Greenberg, L., and Barling, J. 1999. “Predicting Employee Aggression Against Coworkers, Subordinates and Supervisors: The


Minor, W. 1981. “Techniques of Neutralization: A Reconceptuali-


About the Authors

Robert Willison is a senior lecturer at Newcastle University Business School, Newcastle University. He earned his Ph.D. in IS from the London School of Economics and Political Science. He has served as a guest associate editor for MIS Quarterly and a guest editor for European Journal of Information Systems. His work has appeared in European Journal of Information Systems, Information and Organization, Information and Management, Information Technology and People, and Communications of the ACM. His broad area of research is IS security, with a focus on employee computer abuse.

Merrill Warkentin is professor of MIS and the Richard Puckett Notable Scholar in the College of Business at Mississippi State University. He earned his Ph.D. in MIS at the University of Nebraska–Lincoln. His research, which focuses on Information Systems Security, Electronic Group Collaboration, and eCommerce, has appeared in MIS Quarterly, Decision Sciences, European Journal of Information Systems, Decision Support Systems, and other journals and in numerous books. He is serving as an associate editor for MIS Quarterly, European Journal of Information Systems, and Information & Management, has been a guest editor for special issues in four journals, is the AIS Department Editor for Security & Privacy, and has chaired several international conferences. His work has been supported by the U.S. Navy, NSA, the IRS, the UN, Homeland Security, IBM, and others. He has been a visiting scholar at over two dozen universities in eight nations, served as an ACM National Distinguished Lecturer, and has been a featured speaker at over 100 academic and industry meetings.