DISSERTATION

AN EXPLORATORY INVESTIGATION OF ORGANIZATIONAL SECURITY CLIMATE IN A HIGHLY REGULATED ENVIRONMENT

Submitted by

Edward George Bitzer, III

Department of Psychology

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2010

Doctoral Committee:

Department Chair: Ernest L. Chavez

Adviser: Peter Y. Chen

Benjamin A. Clegg
Jacob E. Hautaluoma
Robert M. Lawrence

ABSTRACT

AN EXPLORATORY INVESTIGATION OF ORGANIZATIONAL SECURITY CLIMATE IN A HIGHLY REGULATED ENVIRONMENT

Security professionals, particularly those working in the field of nuclear security, have become increasingly interested in organizational characteristics which might influence an organization's security performance. However, empirical research on such constructs has been limited. Therefore, the purpose of this project was to conduct an exploratory investigation of the proposed construct of security climate. In light of the limited amount of previous work on the topic the study sought to operationalize the construct, establish the emergent nature of the construct, and investigate the impact of security climate on security performance.

The participating organization, which operates in the highly regulated nuclear environment, provided three years of archival data gathered from multiple divisions within the enterprise. Results indicate that security climate is a multidimensional construct comprised of management support for security, co-worker support for security, and security policies and procedures. Evidence also suggests that individuals' perceptions regarding security do become shared among employees within the same unit which verifies the emergent nature of security climate. Furthermore, security climate varied across units and these differences were correlated to division security exposure.

However, the hypothesized relationship between security climate and security performance, after controlling for security exposure, could not be accurately assessed due to the presence of reciprocal suppression among the security climate and security exposure variables. Nonetheless, zero order correlations did provide some evidence of a relationship between security climate and two separate measures of security performance (event frequency and event severity), although the results were not in the anticipated direction. Implications of the study, as well as directions for future research, are discussed.

Edward George Bitzer, III
Department of Psychology
Colorado State University
Fort Collins, CO 80523
Fall 2010

ACKNOWLEDGEMENTS

This research would not have been possible without the support and assistance I have received from so many incredible individuals along the way; I am deeply grateful to all of those who generously shared their talents and expertise with me. And while it isn't possible to individually recognize all of these contributions, I would be remiss not to mention a few people who have been absolutely integral to the completion of this work.

First I would like to extend a special thank you to my advisor, Peter Chen, whose contributions to this project cannot be overstated. Thank you for sharing your wisdom and your patience. Thank you for challenging me and encouraging me. Without question, your guidance has made this research better. More importantly, your guidance has made me better. For that I will always be indebted to you. I've been lucky to have you as an advisor, and honored to have you as a friend.

I would also like to thank my committee members – Ben Clegg, Jack Hautaluoma, and Bob Lawrence – whose comments and suggestions helped to shape my thinking on this topic. The unique perspectives each of you brought to this effort have been invaluable. Thank you all.

I must also thank Roger Johnston for starting me down this path and supporting me at every turn. The opportunity to work with someone as creative and open minded as you has been a true pleasure. I hope you have had as much fun working with a psychologist as I have had working with a physicist.

My thanks also go to Lisa Guiterrez, who opened all the right doors for me. Without you, this project would have died before it even got started. Likewise, I am grateful to Roger Hagengruber, Jack Killeen, Andy Budka, and Ginny Melvin for their willingness to listen to a budding idea and their generosity in helping me make it a reality. You and your teams are true professionals, and we are all better off because of it.

For Mom and Dad

Through the years I've been fortunate to have many great teachers. But none have taught me more, in the subjects that really matter, than the two of you. I wish I had taken better notes.

and

For Rita and Jonathan

We've laughed with each other and cried with each other, fought with each other and fought for each other. I'm truly blessed to have that one constant … we have always had each other.

I LOVE YOU ALL!

TABLE OF CONTENTS

LIST OF TABLES

An Exploratory Investigation of Organizational Security Climate in a Highly Regulated Environment

Security – which can be defined as the act of "safeguarding (the interests of) a state, organization, person, etc., against danger" (Simpson & Weiner, 1989) – is an extremely broad concept given its applicability at so many levels of society. As the definition implies, entities from the individual to the nation state – and perhaps even the global community – are faced with potentially harmful security threats. Organizations are no exception. Virtually every organization must confront a variety of threats that can have dire consequences for the organization, its members, and the broader society. Consider the following examples:

- Studies suggest that 75% of employees steal from their employer at least once (Case, 2000; McGurn, 1988) and almost 95% of U.S. business have reported experiencing some theft or fraud (Case, 2000). And while some businesses in industries such as Retail may factor some employee theft into the "cost" of doing business, the possibly severe consequences of such acts become clear when one considers that an estimated 20% (Coffin, 2003) to 30% (Morgenstern, 1977) of U.S. business failures come as a direct result of employee theft and dishonesty.
- Workplace violence is a remarkably common problem faced by many organizations. So common, in fact, that one study found nearly 25% of organizations surveyed reported some type of physical attack against an on-the-job employee during the course of a three year period (Rigdon, 1994). Although media attention typically

focuses on the tragic cases of workplace violence that result in fatalities, even non-fatal (but more frequent) incidents can have grave impacts on an organization and its employees.

- The widespread adoption of information technology has introduced organizations to a number of potential security threats including electronic espionage, denial of service attacks, and even identity theft. A variety of recent media reports highlight such problems and underscore the need to protect both computer networks (e.g., McGregor & Sevastopulo, 2007; Marquand & Arnoldy, 2007) as well as information stored on electronic media (e.g., Lee, 2006; Seper, 2007). As organizations continue to expand their reliance on information technology, the importance of computer security will continue to grow.

Theft, violence, and computer hacking are just three examples from a long list of security threats which confront organizations. In light of the potentially severe impacts any one of these threats can create, organizations are increasingly viewing strong security as an operational necessity that is vital to their long term interests. This is particularly true in Western industrialized countries such as the United States. In fact, a report published by the Federal Reserve Bank of New York (Hobijn & Sager, 2007) found that total government and private sector expenditures designated for homeland security[1] rose from $56 billion in 2001 to almost $100 billion in 2005.

Much of this recent interest and investment has been focused on the development of security hardware and software which utilizes advanced technology such as global

[1] Hobijn and Sager used criteria from the Office of Management and Budget to determine government spending and define private sector expenditures in terms of spending on protective services (i.e. guards) and electronic equipment (e.g., cameras, etc.). The authors acknowledge some problems with theses definitions, but they also rightly point out how difficult it is to accurately segment and quantify the security industry.

positioning systems, radio frequency identification tags, sophisticated data encryption algorithms, and computer software and hardware which monitors computer networks for indicators of possible intrusion. Researchers and academicians in fields such as security engineering, cryptography, and computer security have contributed to great advances in such technology and hardware. And while this type of technology can have limitations and vulnerabilities (e.g., Warner & Johnston, 2002; Warner & Johnston, 2006), the proper application of these devices can significantly inprove security. But research (e.g., Pond, 2002) suggests that many security challenges have contributing factors related to human and organizational characteristics, and the deployment of high tech equipment does not always address these root causes. Therefore, in addition to the work of those in fields like security engineering and cryptography, the study of security can also be advanced by examining organizational and individual factors which may affect security practices, security compliance, and/or security behaviors. In the present study, I will examine the characteristics of one organizational variable, security climate, and investigate the variable's usefulness as a predictor of security performance.

Anyone attempting to study security climate is faced with three major challenges. First, there are many different types of workplace security incidents (e.g., theft, sabotage, violence, information leaking, etc.), yet there does not seem to be a single framework for organizing them. Second, the concept of workplace security needs to be distinguished from other potentially similar constructs such as workplace safety as well as counterproductive workplace behaviors (CWBs, Spector, 1975) and other related terms (deviant workplace behaviors, Robinson, & Bennett, 1995; workplace violence or workplace aggression, Neuman, & Baron, 1998). Finally, the concept of security climate

has gone largely unexplored and therefore must be operationalized in a meaningful way. In the following sections, an attempt will be made to begin to address these challenges.

A Framework for Understanding Workplace Security Incidents

Based upon a review of one organization's internal security incident reports as well as literature that examines various proposed taxonomies of workplace aggression (Snyder, Chen, Grubb, Roberts, Sauter, & Swanson, 2004), a basic framework for organizing and categorizing workplace security incidents is suggested here. Within this framework, security incidents are categorized based on three primary dimensions - perpetrator, target, and intention. First, security threats are the result of individuals' violation (for whatever reasons or motivations) of security rules. These people can be affiliated with organizations or not. In other words, workplace security incidents (e.g., information leaking) can be caused by organizational insiders, organizational outsiders, or a combination of the two.

The second dimension that can be used for categorizing security incidents is based on the nature of the asset being threatened. While there may be other ways to categorize assets (for example, one common distinction among security professionals is between physical assets vs. computer/electronic assets), this framework does so based on a continuum from organizational assets to individual assets. Obviously an organization is motivated to protect the assets it owns from threats like theft or vandalism, but it should also be concerned by threats to individual employees such as theft of personal property or workplace violence.

The third dimension for categorizing security incidents at work is the intent of the perpetrator. In some cases, security incidents (such as espionage, sabotage, and

physically or verbally attacking co-workers) occur as the result of intentional actions on the part of the perpetrator. However, in some circumstances, security incidents occur unintentionally due to negligence or the lack of awareness. For instance, when employees inadvertently transmit sensitive organizational information to unauthorized individuals or accidentally leave secure entryways unlocked and unprotected. Although incidents of this type are likely to threaten organizational assets, there is no malicious intention to harm the organization.

Workplace Security, Counterproductive Workplace Behaviors, and Workplace Safety

While the above framework may be useful for categorizing various types of security incidents, it is particularly relevant to this study because it provides information which may help to identify similarities and differences between security and two other related constructs: counterproductive workplace behavior (CWBs) and workplace safety. These two constructs are noteworthy because even though it will be argued that both are distinct from security, both are related to – and in some cases overlap with – the security construct.

The CWB construct, which was initially proposed by Spector (1975), has been defined as "any intentional behavior on the part of an organization member viewed by the organization as contrary to its legitimate interests" (Sackett, 2002, p. 5). It is a broad concept that encompasses perhaps as many as eighty-five different types of behaviors (Gruys, 1999). From an organization's perspective, CWBs include aggression, hostility, sabotage, theft, violence, and withholding of output. CWBs can be expressed overtly or covertly as well as physically or verbally. Over the years, researchers have proposed and defined a number of constructs (including antisocial workplace behavior, deviance,

bullying, and organizational aggression) which, despite some minor distinctions, tend to be very closely related to the CWB construct. In fact, the definitions for each of these terms share two common elements. First of all, these behaviors are committed by perpetrators with the intention to negatively impact other employees or their employers. Second, these behaviors may be committed for a variety of different reasons which suggests that the concept is not a unitary one (Spector, Fox, Penney, Bruursema, Goh, & Kessler, 2006).

Considering the broad nature of the CWB construct, one might argue that workplace security is merely a subset of the CWB construct. However, this study does not conceptualize CWBs and security as synonymous concepts. First, research on CWBs has exclusively focused on the actions of organizational members but security threats can be the result of organizational insiders as well as outsiders and security regulations are often developed with the specific goal of deterring both categories of perpetrator. Furthermore, CWBs have traditionally been defined in a way that includes intentional acts but excludes any unintentional behaviors. While many security incidents are the result of a malicious perpetrator acting with intent, the occurrence of a security event is often the result of a number of contributing factors which could include unintentional acts (e.g., errors) on the part of an employee which creates a vulnerability that an adversary could exploit.

Another construct similar to workplace security is workplace safety. In some societies there is very little distinction between safety and security. An example of such a culture is Russia, where the similarity between the two constructs is reflected linguistically by the fact that the same word is used to represent both concepts

(Khripunov, 2005). And while the English language does have separate words for the two concepts, many English language thesauri list safety and security as synonyms (Kipfer, 2007). However, the relationship between the two concepts is more than just a matter of linguistics. For example, programs that support either safety or security tend to be largely compliance-based (i.e. rules driven). In addition, the causes of both safety and security events can often be traced back to multiple contributing factors.

To demonstrate the similarity between safety and security, consider an instance of workplace violence as an example. Because workplace violence can result in physical and emotional harm to an employee, clearly such events present safety concerns for an organization. However, organizational efforts to prevent such events, as well as respond to them when they are occurring, are likely to fall within the responsibilities of the organization's security professionals. The fact that a single event can span both the safety and security fields illustrates the close relationship between the two constructs.

Nonetheless, workplace safety is conceptually different from workplace security on several grounds. First, workplace safety research and legislation (e.g., Occupational Safety and Health Act, 1970) has mainly focused on establishing safe and healthy working conditions for employees by reducing illness as well as fatal and non-fatal injuries resulting from inadequate working conductions. In other words, safety threats such as hazard exposures are almost exclusively directed at individual workers. In contrast, the framework for understanding security presented earlier incorporates threats to the individual as well as the organization. Second, threats to workplace safety are not typically the result of intentional acts by employees nor caused by a malicious adversary; rather, they are often the result of characteristics of the job tasks and working conditions.

Security incidents, on the other hand, can be committed intentionally or unintentionally, with or without an adversary. Finally, security officers and safety officers perform different tasks with different tools and equipment (O*NET, Department of Labor).

Despite the differences between security and the constructs of CWBs and safety, the similarities which exist may support the notion that results and conclusions from research on these other topics may have some applicability to the field of organizational security. For example, Hollinger (1986) found that CWBs such as theft are more common among younger employees with less tenure and less commitment to the organization, a finding that is clearly relevant to the field of security. And while much of the CWB research tends to focus on individual variables like those in Hollinger's study, Trevino and Youngblood (1990) have suggested that more attention should be paid to situational variables. This suggestion has begun to gain traction in the field of security as well.

The idea of applying the construct of organizational culture, defined as a phenomenon based on symbolic meanings that reflect core values and underlying ideologies and assumptions (Ostroff, Kinicki, & Tamkins, 2003), to the field of security has received increased attention in recent years. This is especially true in the field of nuclear security, which is focused on the protection of nuclear assets (such as fissile materials, technology, and facilities) used for research, power generation, and military purposes. For instance, the International Atomic Energy Agency (IAEA), which is an agency of the United Nations responsible for monitoring nuclear security and safeguards programs among member nations, has repeatedly issued statements urging members to foster a good nuclear security culture as a supplement to existing efforts to protect

nuclear assets (e.g., IAEA, 2001; IAEA, 2002; IAEA, 2003). In addition, the presidents of the United States and Russia have issued a joint statement that acknowledges the importance of nuclear security culture and commits to developing both a greater understanding and increased application of the construct (White House, 2005). But it must be acknowledged that the concept of nuclear security culture is still very much in its infancy. To date, the IAEA has not offered any concrete guidance on what nuclear security culture really means, how it could be established, or what impact it may have on nuclear security efforts. And despite presidential support, theoretical and empirical investigations of the construct have been limited. Ultimately, though, this high-level interest in the topic is encouraging and will likely lead to more extensive research attention in the future.

However, organizational culture is not the only organizational variable with potential applicability to security which merits more extensive research attention. The closely related construct of organizational climate – defined as attributes of organizations that are reflected by employees' shared perceptions of organizational policies, practices, and procedures about specific organizational focus areas (Reichers & Schneider, 1990; Schneider & Snyder, 1975) – may also be a useful addition to the field. But in contrast to organizational culture, the potential for applying organizational climate to the field of security (and more specifically nuclear security) has gone largely unaddressed. In light of this void, the purpose of the current study is to begin the process of developing and validating the construct of security climate.

Organizational Climate

As defined previously, organizational climate has been conceptualized as characteristics or attributes of organizations that are reflected by employees' shared perceptions of organizational policies, practices, and procedures about specific organizational focus areas (Reichers & Schneider, 1990; Schneider & Snyder, 1975). The construct, which has had a long history in the behavioral sciences, has evolved quite substantially since its inception. While a thorough review of this evolution is beyond the scope of this study (cf. Reichers & Schneider, 1990), a brief summary will be helpful for understanding the development of workplace security climate in the later section.

The origins of organizational climate can be traced back to the work of Kurt Lewin and colleagues starting in the late 1930's. Lewin, Lippitt, and White (1939), introduced the term climate, which they also called atmosphere, in a study of adolescent boys at a summer camp. In the thirty to forty years that followed the work of Lewin et al., the study of organizational climate has gained widespread favor. Initially, organizational climate was viewed as a global, almost all-purpose, construct that could be used to study a wide array of organizational events. However, a series of reviews (e.g., Campbell, Dunnette, Lawler, & Weick, 1970; Payne & Pugh, 1976) have suggested that the construct of organizational climate has only a limited impact on any one type of organizational outcome. Specifically, researchers have argued that the general conceptualization of organizational climate would not be helpful in predicting or influencing specific phenomena such as managerial job performance in organizations (Pritchard & Karasick, 1973). This, in part, led Schneider (1975) to conclude that the general concept of organizational climate had become so all-encompassing that it was no

longer useful. Therefore, Schneider suggested that future climate studies should identify a specific and focused area of concern, a "climate for" something. This suggestion has been widely accepted and a number of specific climates – such as climate for service (Schneider, 1990), climate for safety (Zohar, 1980), climate for creativity (Amabile, Conti, Coon, Lazenby, & Herron, 1996), and climate for technical updating (Kozlowski & Klein, 1987) – have been proposed and studied. But despite these diverse applications of the construct, each of these climate types share the common understanding that climate is an organizational characteristic represented by employees' shared perceptions regarding a specific and focused area of organizational concern. The current study also shares this view of climate and therefore will focus on organizational climate for security (or workplace security climate), rather than generic organizational climate, in order to better understand workplace security.

Definition and Dimensions of Workplace Security Climate

By adapting the definition of general organizational climate for use with the strategic outcome of security, workplace security climate can be defined as a security characteristic of an organization that is manifested in employees' shared perceptions of the organization's security policies, practices, and procedures. In this section, the dimensional nature of security climate, the phenomenon of security climate emergence within organizations, and individual and organizational outcomes associated with security climate will be discussed.

The current study views security climate as a multifaceted construct, a view which is aligned with the way most of the previously proposed types of organizational climate have been viewed. Rather than a homogeneous perceptual domain, the construct

is comprised of a number of separate dimensions. These dimensions can be viewed as distinct categories of employee perceptions formed in response to sets of security-related stimuli that are encountered in the work environment. As a result, research on security climate should explore the possible dimensions that make up the construct.

Over the years, climate researchers have proposed many climate dimensions including structure, reward, risk, warmth, support, standards, conflict, identity, democraticness, supportiveness, innovativeness, peer relations, pressure, and so on (Ostroff et al., 2003). However, this process of identifying climate dimensions has generally lacked an organized framework for generating these dimensions which has lead to inconsistency and confusion in the way different dimensions are labeled, defined, and used (Carr, Schmidt, Ford, & DeShon, 2003). Most, if not all, of the empirical research related to climate dimensions relies primarily on factor analytic techniques (Meyer, 1968; Schneider & Bartlett, 1968; Schneider & Hall, 1972; Thornton, 1969; Waters, Roach, & Batlis, 1974), which has resulted in paring the number of climate dimensions to between four and seven. For example, Waters et al. identified four climate dimensions including effective organizational structure, close impersonal supervision, open challenging environment, and management and peer support.

One frequently cited work attempting to organize the dimensions of climate is that of Campbell, Dunnette, Lawler, and Weick (1970). Campbell et al. reviewed a small sample of climate research from the 1960's and found that there were four common dimensions that appeared in each study. These dimensions included individual autonomy, structure imposed upon the position, reward orientation, and consideration/warmth/support. While interesting, the authors urged caution when trying

to draw conclusions from this finding. Not only were the findings based on a limited number of studies (four), but the authors also found a number of examples of proposed climate dimensions from one or more of these studies that were not included in the others. Despite these shortcomings, the work of Campbell et al., Waters et al. (1974), as well as research on safety climate has helped to lay the groundwork for the development of security climate dimensions.

Management Support

One dimension worthy of consideration for inclusion as a dimension of security climate is the dimension of management support. As a dimension examined in previous climate studies (e.g., Zohar, 1980, 2000, 2002; Hemingway & Smith, 1999; Smith-Crowe, Burke, & Landis, 2003; Tracey & Tews, 2005; Weyman, Clarke, & Cox, 2003), management support has previously been defined as employees' perceptions of the degree to which managers and supervisors support, promote, manage and prioritize the importance of various organizational outcomes. Perceptions of management actions that demonstrate commitment to a particular outcome (such as security in the present study) are important because they may influence employee's perceptions of the overall importance of that outcome to the organization. For example, Clarke (1999) found that the discrepancy between managers' espoused values (those that are officially endorsed) and managers' enacted values (those that are put into practice through actual behavior) about safety was a driving factor in the development of employee perceptions of a safety program. Clarke's conclusion about the importance of management commitment is supported by a number of other safety climate researchers. At least three studies (Flin, Mearns, O'Connor & Bryden, 2000; Ho, 2005; Seo, Torabi, Blair, & Ellis, 2004) have

been conducted which explore commonalities among various operationalizations of the safety climate construct. Results from each of these reviews suggest that the most commonly used dimension in the field of safety climate is that of management support. For example, Flin et al. found that of the eighteen scales of safety climate included in their review, 72% contained some measure of management commitment or support for safety. This result was supported by Seo et al. who found that among the sixteen studies reviewed nearly two-thirds operationalized management commitment or support as a dimension of safety climate.

One possible explanation for the importance of management support comes from social exchange theory (Blau, 1964; Homans, 1958). Social exchange theory suggests that when one party in a social interaction consistently acts in a way that benefits another party, the latter party will eventually adjust their own behavior in a way that benefits the former. Hofmann and colleagues (Hofmann & Morgeson, 1999; Hofmann, Morgeson, & Gerras, 2003) have suggested a social exchange model as the theoretical mechanism underlying the significance of management commitment as a dimension of safety climate. According to these authors, when employees perceive strong management commitment to safety they return that commitment with safety compliance as part of the social exchange. It is possible that the same type of mechanism underlies the management commitment dimension of security climate.

Effects of management support or commitment on security behaviors might also be explained by role modeling. Greenberg and Scott (1996) have suggested that at least some employee theft may be attributed to the fact that employees mimic behaviors modeled by their supervisors or managers. They argued that when a manager engages in

activities such as theft, employees would likely perceive that managers aren't committed to security and therefore it is not important for them to be concerned with it either. Although there is a lack of empirical evidence testing the above proposition, such a suggestion is supported by assertions from a number other experts on employee theft (e.g., Cherrington & Cherrington, 1985; Greenberg, 1997; and Hollinger, 1989).

Further evidence for the importance of management support for security comes from research suggesting that certain actions of managers convey their commitment to security, which in turn influences employees' security behaviors. For instance, inappropriate security behaviors such as employee theft diminish when managers regularly communicate to employees about the importance of security (Carter, Holmström, Simpanen, & Melin, 1988). In addition, it has been suggested that when managers conduct regular security audits they are displaying their commitment to security, and this practice can lead to a reduction of employee theft behaviors as well as raise management's awareness of the problem (Jones and Terris, 1983). Finally, a limited amount of theoretical work in the field of nuclear security culture also suggests that management support for security is an important dimension of security climate. For example, Khripunov, Nikonov, and Katsva (2004) contended that managers "can use their positions of power to…encourage new and different assumptions and patterns of thinking among their colleagues…" (pp. 45-46). In fact, these authors state that one of the key attributes of top leaders in the nuclear field is a "personal commitment to security culture" (p. 47).

In light of these research findings, the following hypothesis is proposed:

H1a: Perceptions of management support for security is a dimension of security climate.

Co-Worker Support

Co-worker support for security (which the study defines as employees' perceptions of the degree to which co-workers and peers support, promote, and prioritize the importance of organizational security) is another potentially important dimension of security climate. The idea that co-worker support for security would impact an individual's security behavior is not without merit. Research has shown that when people come together in groups, rules of behavior (often referred to as norms) develop quickly, are usually very clear to group members, and can profoundly impact member behavior (Tuckman, 1965).

Additional theoretical support for the importance of co-worker support as a dimension of security climate, and the role this dimension might have on an individual's behavior, comes from the theory of reasoned action (Fishbein & Ajzen, 1975) as well as a subsequent refinement in that theory which Ajzen (1985; 1991) has called the theory of planned behavior. Both of these theories propose that an individual's behavior is impacted by social influence in the form of both subjective norms as well as normative beliefs. On the one hand, subjective norms consist of perceptions that a behavior, in this case a behavior either supportive of or detrimental to security, is expected by important and respected people (such as co-workers) that surround an individual. On the other hand, normative beliefs are an individual's perceptions about a behavior (again, either supportive of or detrimental to security) that are influenced in part by the judgments of the significant others that surround the individual (such as co-workers). Taken together, subjective norms and normative beliefs can exert social influence from one's co-workers.

These social influences can then impact an individual's perceptions, as well as behaviors, related to security.

Work in the area of CWB's also seems to suggest that co-work support may be an important component of security climate. A number of studies of employee theft in various industrial settings (Horning, 1970; Sieh, 1987) have found that in situations where there was no clear guidance from the organization about the taking of company property, work groups established their own norms about what was appropriate and inappropriate behavior. However, even in situations where the organization has provided clear standards of behavior, group norms often supersede such rules. For example Dabney (1995) studied co-worker norms among nurses working in a hospital setting. This study found that even when the hospital had explicit rules against taking any medicine from hospital supplies for personal use, nurses had developed their own norms which individuals used to rationalize the taking of certain types of drugs such as non-narcotic pain medicines. However, these group norms were in line with some hospital rules such as strictly forbidding the taking of any narcotic medications. In fact, group norms have not only shown to be more influential than formal organizational rules, but it has been suggested that it is only through group norms that formal rules are enforced (Hollinger & Clark, 1982).

Given this literature, the following research hypothesis is put forth:

H1b: Perceptions of co-worker support for security is a dimension of security climate.

Perceptions of Security Policies and Procedures

It has been argued that perceptions of an organization's policies and procedures are a key component of climate (Rentsch, 1990). Zohar (1980) found that, along with

management support, employees' perceptions of safety procedures were an important aspect of an organization's safety climate. In addition, Coyle, Sleeman, and Adams (1995) found that employees' perceptions of company safety policies accounted for the second largest percentage of variance in safety climate among clerical and service organizations in Australia. Similarly, Diaz and Cabrera (1997) found that perceptions of organizational policies explained the greatest percentage of variance in safety climate among employees working in the airline industry.

While limited, research in the field of security also suggests that security policies and procedures are often judged by employees in terms of their relevance (are they necessary?), their effectiveness (do they actually improve security?), and their user-friendliness (are they understandable and not overly cumbersome to implement?). As such, Khripunov et al. (2004) suggested that security policies and procedures should be up-to-date, succinct, clear, and user-friendly.

In light of the central role employees' perceptions of security policies and procedures play in the definition of security climate, the following research hypothesis is proposed:

H1c: Perceptions of security policies and procedures are a dimension of security climate.

Emergence of Security Climate

Security climate reflects employees' shared perceptions about workplace security. The formation of climate, which is called climate emergence, occurs when individual perceptions become shared at the group level. Three main theories have been put forth in the organizational climate literature to explain the mechanisms driving climate emergence. First, the structrualist perspective (e.g., Payne & Pugh, 1976) suggests that

organizational characteristics such as structure or size create a strong situation that leads employees to develop similar types of perceptions. The attraction-selection-attrition perspective (e.g., Schneider & Reichers, 1983) suggests that individuals are attracted to organizations that seem to match their personality, organizations tend to select individuals with personalities that fit with the organization, and when an individual joins and organization that is a mismatch for their personality they will ultimately leave whether voluntarily or otherwise. In the end, this process will result in a somewhat homogeneous workforce that tends to develop similar types of perceptions. Finally, the socialization perspective (e.g., Ashforth, 1985) suggests that when newcomers are socialized into a group, and as group members interact over time, a level of conformity develops which leads to consistency in the perceptions that employees develop.

While each of these theories has seen some research attention, there is still no overwhelming empirical support in favor of any of these theories over the others. But despite the lack of a universally accepted explanation for the mechanisms driving the emergent process, evidence suggests that organizational climate in the form of shared perceptions does emerge within organizations. For instance, Zohar (1980) administered a safety climate survey to a sample of employees from twenty different factories representing four industry segments to investigate whether safety climate would emerge among the employees within each of these organizations. His results suggested that shared safety perceptions did exist within individual factories.

Although Zohar studied safety climate by assessing the level of agreement among individuals within a single organization, the emergence of organizational climate might also occur within distinct units, groups, or departments of a single organization (e.g.,

Zohar, 2000, 2002). This is particularly relevant to the current study because the data was gathered from a very large organization which is made up of a number of divisions. And all of these divisions are distinct from the others in a number of different ways. When viewing these differences within the context of the three theories of climate emergence, investigating security climate at the division level may be merited. For example, differences in size, work environments (laboratories vs. offices), and type of work (business services vs. R&D) might be important in light of the structrualist perspective. The attraction-selection-attrition perspective might be important in light of the fact that many R&D divisions focus on a specific technical field (e.g., physics, chemistry, biology) so many employees within the same division hail from the same academic traditions. Finally, the socialization perspective might be relevant because the organization encompasses a very large campus taking up tens of square miles and divisions tend to be separated from each other geographically throughout the campus providing limited opportunities for interaction among employees in different divisions.

Based upon these and other distinctions, any or all of the emergent processes discussed may lead to the emergence of security climate at the division, rather than organization, level. Therefore, the following hypothesis is proposed:

H2a: Security climate is shared among employees within the same division.

In addition to studying the emergence of safety climate within a single organization, Zohar (1980) also investigated whether shared safety perceptions varied between organizations in different industries. His results suggested that safety climate varied among organizations employing different kinds of technologies that presented different levels of risk. The combination of shared perceptions within individual

organizations and safety climate variations between organizations with different levels of risk led him to conclude that "a definable safety climate" (p. 99) existed within these organizations.

In support of Zohar's findings, a number of studies in the field have found that safety risk is related to the type of safety climate that exists within an organization. For example, Cree and Kelloway (1997) found that employees' perceptions of co-worker commitment to safety (a dimension of safety climate) predicted employees' risk perceptions in a manufacturing environment. Likewise, Huang and colleagues (Huang, Chen, DeArmond, Cigularov, & Chen, 2007) found that safety climate was negatively related to employees' perceptions of injury risk. However, this relationship was moderated by employees' work shift.

In addition to the differences between divisions mentioned previously, one significant difference between divisions concerns the amount of classified or sensitive work that is done. Almost all of the work conducted in some divisions is of a classified or sensitive nature, some divisions conduct very little of this type of work, and many divisions fall somewhere between these two extremes. The fact that divisions vary in the amount of classified work conducted creates inequity in the level of security exposure, or risk, they face. If security climate does emerge at the division level (H2a) and division security climate is related to a division's security risk, than the current study would be able to conclude, as Zohar did with safety climate, that a "definable security climate" exists within each division. Therefore, the following hypothesis is proposed:

H2b: Division security climate will be related to division security exposure.

Outcomes of Security Climate

Much of the interest in the construct of organizational climate is the result of efforts to better understand and improve organizational performance in some form or another. And while results have been somewhat mixed, recent research has discovered significant relationships between climate and performance. For example, Zohar (2000, 2002) found a relationship between safety climate and organizational injury rates. In addition, customer service climate has been found to predict customers' ratings of service quality (Schneider, White, & Paul, 1998).

The expected effects of organizational climate on organizational performance generally rest on two core assumptions about employees within an organization (Schneider, 1975): "(1) humans attempt to apprehend order in their environment and to create order through thought; and (2) humans apprehend and/or attempt to create order in their environment so they can effectively adapt their behavior to the work environment" (p. 447). The first assumption implies that employees desire, create, and maintain order in their workplace. The second assumption implies that an ordered workplace helps employees determine what behaviors are appropriate in a given situation.

In the context of security, employees comprehend order through security rules or practices regarding appropriate behavior. They then adjust their actions in accordance with the order created at work. In this way, when a positive security climate exists, employees are able to adjust their actions in a way that supports the security goals of the organization. As a result, enhanced organizational security performance is expected in an organization with a strong security climate.

The current study sought to investigate this security climate-security performance relationship. To do so, empirical measures of security performance had to be identified. One of the clearest indicators of an organization's security performance is security event frequency. Event frequency is simply the number of security events (standardized based on division size) that occur within a particular division over the course of a set time period. This metric, similar to the use of injury rates when studying safety climate, is the primary measure of security performance used by many organizations.

However, testing the security climate-event frequency relationship might be complicated by the divisional differences in security exposure described above. This possibility is supported by years of research in the safety field. In fact, Zohar (2000) points out that the importance of controlling for risk in the safety field was recognized at least as early as the 1930s when Heinrich (1931) proposed a model of industrial accidents. This model suggested that the probability of an accident was determined by the confluence of both unsafe behaviors as well as unsafe conditions. This second contributing factor constitutes risk and is analogous to security exposure in the current study.

Unfortunately, some research from the field of occupational safety suggests that the relationship between risk and outcome is not so clear cut. On the one hand, in a study of foundry workers at two different plants, Guastello and Guastello (1988) found that individuals working in the plant who used more hazardous equipment identified more risks associated with their work. However, the high risk plant also experienced fewer accidents than employees working in a second plant that used less hazardous equipment. This result was attributed, in part, to the fact that employees in the higher risk – lower

accident rate plant were more experienced and better able to identify safety risks than those in the second plant.

Despite this counterintuitive finding, there is ample reason to believe that risk has some relationship to outcomes when considering safety as well as security. As such, it is prudent to control for security exposure in the current study. With that in mind, the following research hypothesis regarding the security climate – security performance relationship is posited:

H3a: Security climate will be negatively related to frequency of security events, after controlling for level of security exposure.

And while the frequency of security events is an important metric, it is not the only useful indicator of organizational security performance. This is illustrated by the fact that some security events may be much more severe than others. So even if two organizations experience the same number of events, their security performance isn't the same if one organization experiences events that are more severe. Therefore incident severity, which can be determined by the consequences or damage caused, is another important indicator of an organization's security performance. As such, the following research hypothesis is put forth:

H3b: Security climate will be negatively related to severity of security events, after controlling for level of security exposure.

Summary of Research Propositions

Due to the lack of research on security climate, the present study seeks to 1) develop the construct, 2) determine if climate does emerge within an organization and its sub-units, and 3) explore the relationship between security climate and security

performance. To address the first goal, the following three research propositions have been put forth:

H1a: Perceptions of management support for security is a dimension of security climate

H1b: Perceptions of co-worker support for security is a dimension of security climate.

H1c: Perceptions of security policies and procedures are a dimension of security climate.

To address the second goal, the following research propositions have been put forth:

H2a: Security climate is shared among employees within the same division.

H2b: Division security climate will be related to division security exposure.

To address the third goal, the following two research propositions have been put forth:

H3a: Security climate will be negatively related to frequency of security events, after controlling for level of security exposure.

H3b: Security climate will be negatively related to severity of security events, after controlling for level of security exposure.

Method

Background of the Studied Organization

After extensive discussions with its senior security managers, a large (primarily federally funded) research and development laboratory agreed to participate in this research by providing secondary data for use in the study. The organization, which employs approximately 10,000 people either directly or through sub-contractors, operates as part of the United States Department of Energy (DoE). And while the assets of the organization (e.g., facilities, equipment, etc.) are owned by the DoE, the operations and management of the laboratory is contracted out to a third party institution.

The work conducted at the laboratory spans a wide range of academic and technical fields. But despite this diversity, most of the work that is done is aligned with the organization's primary mission of applying science and technology to address the challenging problems of national security. Given the nature of this type of work, the organization is faced with numerous security concerns that range from everyday issues common to any organization operating today (e.g., petty theft by employees) to the most serious of threats common only to the few organizations that routinely deal with sensitive and classified information or technology (e.g., espionage by agents of a foreign government).

As a result, it is not surprising that the organization places a great deal of emphasis on maintaining the highest level of security. For example, the organization has an extensive set of security procedures which govern many aspects of the work

environment, new employees (even those who will never have access to sensitive information) go through rigorous background screening prior to beginning work, and existing employees are required to complete regular security training and refresher courses. In addition, the organization utilizes cutting edge security technologies and maintains a full-time, well-trained, and extremely professional force of security officers. In light of characteristics such as these, the organization presents a unique opportunity to study the construct of security climate in a highly regulated environment.

Data Sets Used in the Current Study

The data used in the current study were extracted in four separate data sets which were provided by the organization. While information from the first data set was analyzed separately from the others, the three remaining data sets included division identification as the single piece of demographic information. Therefore, it was possible to aggregate data within each data set based on the divisional structure of the organization and then connect the three data sets at this level. And although this demographic data made it possible to analyze the data sets at the division level, the rationale for doing so went beyond mere convenience. First, the construct of organizational climate has traditionally been viewed as a group level variable as opposed to psychological climate which is conceptualized as an individual level variable (e.g., James and Jones, 1974). In addition, divisions have an ample sample size of responses to the employee opinion survey as well as a base rate of security events that is high enough to conduct meaningful analyses. Also, data at the division level contained sufficient variability given that divisions are all distinct from each other along a number of factors including the nature of their work (e.g., physics, chemistry, biology) and their geographic location (lab and

office space is spread out over many square miles making interaction between divisions less common). Finally, some managers within the organization had expressed concerns about anonymity, and some of the data used in the study was simply unavailable at the individual level. In light of these factors, analysis at the division level was deemed appropriate. Each of these four data sets is briefly described below.

Subject matter expert (SME) data set. The first data set, referred to as the SME data set, consisted of qualitative data compiled as part of a review of business practices designed to better understand the impact of organizational dynamics on security performance. The qualitative data was collected during interviews with ten employees of the organization who were identified by senior security managers as subject matter experts (SMEs) in security. Eighty percent of the SMEs were male and 20% were female. The SMEs had an average tenure with the organization of 14 years 4 months and an average of 18 years 7 months experience in the security field.

The interviews consisted of a structured set of open-ended questions which were designed to probe the effect that a variety of organizational characteristics might have on the organization's overall security performance. Some of the topics addressed in the interviews included behaviors of senior managers, behaviors of direct supervisors, co-worker behaviors, security policies and procedures, the effectiveness of security professionals, and conflicts between security and job demands. SME responses to each question were recorded by hand, as close as possible to verbatim, and were transcribed into a word processing file immediately following each interview. After all the interviews were completed, a total of 141 individual responses were aggregated together to form the SME data set. At that point, both the paper and original electronic transcripts

of the individual SME interviews were destroyed so it was impossible to identify which responses came from which SMEs.

Employee opinion survey (EOS) data set. The second data set, referred to as the EOS data set, consisted of employees' responses to an annual employee opinion survey (EOS) administered by the organization's Human Resources division. Three years of data were included in the EOS data set. In Year One, the survey contained 49 questions assessing employees' opinions on a wide range of topics such as security, safety, and job satisfaction. There were 3694 responses in Year One distributed among 45 divisions (M = 82.09; SD = 86.53) with a total response rate of 43%. In Year Two, the survey contained the same 49 questions. There were 3711 responses in Year Two distributed among 49 divisions (M = 75.73; SD = 76.27) with a total response rate of 45%. In Year Three, the same topic areas were covered but three additional questions were added to the survey for a total of 52 items. Year Three contained 3649 responses distributed among fifty three divisions (M = 68.85; SD = 64.13) for a total response rate of 44%.

Employees responded to the survey questions using a 5-point Likert-type scale ranging from 1 "disagree" to 5 "agree." In addition, employees had the option of selecting a sixth response of "don't know." Responses using this option were treated as missing data. Due to the anonymous nature of the survey it was impossible to track individual respondents from one year to the next, therefore it is possible that survey respondents within each division may or may not be the same from one administration of the survey to the next.

Although a number of demographic questions are included in the employee opinion survey, due to the privacy concerns raised by the laboratory's Human Resources

division the only piece of demographic data included in the EOS data set was the division where each respondent worked. This information was used to aggregate responses on the survey at the division level as well as to connect the aggregated division scores to division level variables in the two remaining data sets. Despite the fact that most demographic information was excluded from the data set, the HR division did provide information about the size of each division in the organization as well as some basic demographic information about the overall laboratory population.

The population from which the EOS data was drawn includes technicians, staff members, and support personnel. Technicians (e.g., welders, fabricators, machinists, etc.) typically have an educational level ranging from high school graduates to those with some college education such as an Associates' Degree. Staff members (e.g., physicists, chemists, mathematicians, etc.) are typically highly educated, generally with at least one graduate degree and most with a Ph.D. Support personnel (e.g., administrative assistants, human resource professionals, accountants, etc.) vary widely in their level of education from high school graduates to those with a Ph.D. Furthermore, the Human Resources Division has indicated that the laboratory traditionally has a very low turnover rate of 3% to 4% per year, although employees may move from one division to another.

Event data set. The third data set, referred to as the Event data set, was provided by the laboratory's Security Division and consisted of information about all of the security events which were reported to the Security Division over a timeframe which overlapped the last two years of data included in the EOS data set. Each security event in the Event data set included information that made it possible to determine which division (or divisions) the security event occurred in, what year it occurred in, and how severe the

event was. Other information, such as whether the event was reported to the Security division by those responsible or by someone else, was also included. This data made it possible to calculate a yearly measure of event frequency as well as event severity for every division included in the study. These data points will be described in greater detail in the measures section.

Exposure data set. Each division varies in the amount of classified and sensitive work it conducts, from those divisions that do almost exclusively this type of work to those divisions that conduct virtually none of this type of work. To account for these differences a fourth and final data set, referred to as the Exposure data set, was provided by the organization. The Exposure data set consisted of a list of each of the divisions within the organization. For each of the divisions, there were five estimates of the percentage of classified and sensitive work conducted within that division. The estimates were provided by five separate security experts, each working independently, who were familiar with the divisions on the list. The SMEs had an average tenure with the organization of 18 years and an average of 24 years 5 months experience in the security field.

Measures

Security climate. Given that there were no a priori dimensions of security climate in the existing empirical climate literature, in order to establish a measure of the construct it was necessary to first identify potential dimensions. Based upon the literature reviewed, three possible dimensions of security climate were identified and defined. These dimensions, along with their definitions, are shown in Table 1. Using these proposed dimensions, six graduate students familiar with the literature on organizational

climate worked independently to sort the interview responses from the SME data set. These students were provided with an electronic file containing instructions for sorting the responses into these three categories as well as a fourth category of Not Applicable (see Appendix A) as well as a table listing the responses which was used to record their sorting results. Agreement among the sorting results from these six judges was calculated as a test of the viability of these security climate dimensions. The findings from these calculations will be reported in the Results section.

Table 1

Proposed Security Climate Dimensions and Definitions

Dimension Name	Dimension Definition
Management Support for Security	Employees' perceptions of the degree to which managers and supervisors support, promote, manage and prioritize the importance of organizational security.
Co-worker Support for Security	Employees' perceptions of the degree to which co-workers and peers support, promote, and prioritize the importance of organizational security.
Perceptions of Policies and Procedures	Employees' perceptions of security policies and procedures including such things as relevance, effectiveness, and user-friendliness.

Based upon the dimensions identified above, a measure of security climate was then developed from the items on the organization's annual employee opinion survey (i.e., the EOS data set). Specifically, following the procedure of Griffin and Neal (2000), three researchers (one advanced graduate student in I/O psychology, one Ph.D. in I/O psychology, and one internationally recognized expert in the security field) independently sorted items from the employee opinion survey into one of the security climate dimensions. If a researcher determined that a survey item did not fit in any of the climate dimensions, it was sorted into a category labeled "Other." After independently sorting each survey item, all three researchers met to discuss their decisions. Any disagreements were discussed until unanimous agreement was reached; if agreement could not be reached the item was dropped from further consideration. The results of this sorting procedure constituted the final security climate measure that was used in the study.

Safety climate. In addition to the security items, the EOS data set also included two items focused on employees' views of safety within the organization. Both of these items assessed employees' perceptions of management support for safety, which was mentioned previously as a common dimension of safety climate (Flin, Mearns, O'Connor & Bryden, 2000; Ho, 2005; Seo, Torabi, Blair, & Ellis, 2004). While safety climate is not a central concern of the research questions in this study, the inclusion of these items made it possible to assess the construct validity of security climate as well as the factor structure of the security climate measure.

Frequency of security events. The frequency of security events was calculated based on data contained in the Event data set which included information about when (month/year) and where (which division or divisions employ the responsible person or

people) each event occurred. This data was used to determine the number of security events that occurred in each division over two separate one-year timeframes, which were defined as the beginning and end of the one-year interval starting when the employee opinion survey was administered. Although the exact date of the survey administration did vary from one year to the next and took place over a two-to-three week period, it was typically started at the beginning of June. Therefore, June 1 was established as the beginning of each year in this study. Specifically, event frequency data for Year Two was calculated based on those events that occurred between June 1st of Year Two and May 31st of Year Three. Likewise, frequency data for Year Three was based on events occurring between June 1st of Year Three and May 31st of the calendar year following Year Three.

It should be noted that the process used in this study for calculating the number of security events that occurred in each division differs somewhat from the process of record keeping used by the organization. As noted, some events result from actions of more than one person and the various individuals sometimes work in different divisions. In such situations the organization will make a determination, based on investigation results, as to where the event should be attributed. After an extensive investigation of each security event, the organization attributes the event to the division that employs the person found to be primarily responsible for the event. While this process may be appropriate for record keeping and auditing purposes, it is insufficient for a study of the relationship between security climate and security performance resulting from employee actions. Specifically, if a security event is the result of actions from multiple employees it is important to account for the actions of every employee involved. Since the

organization's security event database includes enough information to identify the division affiliation of every person deemed to have some responsibility for a security event, even if it isn't the primary responsibility, it is possible to account for the actions of these additional employees. Therefore, for each event in the database, this study credited an event to every division employing someone involved. Specifically, if a security event occurred that was deemed to be primarily the result of actions by an individual in Division A, and to a lesser extent an individual in Division B, both Division A and B were credited with one security event. In order to maintain consistency, if a security event is deemed to be the responsibility of two individuals from the same division, that division was credited for two security events (one for each of the two individuals involved).

However, it would be inappropriate to simply use a raw tally of the number of security events per division as a metric of event frequency. The reason for this is that different divisions within the organization can vary greatly in terms of size, sometimes by a factor of ten or more. As an illustration, consider the case of two hypothetical divisions. The two divisions may be very similar in many ways. In both cases, about 50% of the work done is of a sensitive nature, and the employees of both divisions seem to take their responsibility for security very seriously. Likewise, both divisions experienced five separate security events during a given year. However, one division had 500 employees in that year whereas the other only had 250 employees. If everything about the two divisions is identical, except for the fact that one has twice as many employees as the other, then the laws of probability suggest that the larger division would likely experience twice as many security events as the smaller one over the course of the

same time period. But by only looking at the raw numbers of security events in a given year, it would appear that the two divisions exhibited an equal level of security performance during that time period. It is only when division size is taken into account that the true differences in security performance can be seen.

This is clearly not a groundbreaking concept. In the related field of safety research, it is common to report an organization's accident rate by taking the size of the organization's workforce into consideration (e.g., Silva, Lima, & Baptista, 2004). Therefore, the current study employed a relatively simple process to standardize the security event frequency metric based on division size. That process was simply a matter of dividing a division's raw event frequency tally by the number of employees it has and then multiplying that by 100. This metric conceptualizes a division's event frequency as the number of security events per 100 employees.

Event severity. Event severity refers to the potential impact or damage an event may cause. When the organization becomes aware that a security event has occurred, one of its trained security investigators is assigned to the case. During the course of the investigation, the investigator makes a determination about the severity of the event based on a categorical severity rating system developed by the DoE for use at all of the facilities within the department. This system, called the Impact Measurement Index (IMI), consists of four event categories that have been labeled IMI-1 (the most severe on the scale) through IMI-4 (the least severe on the scale). If the organization's security investigators determine that an event falls into one of these categories, than the organization must report it to the DoE. These IMI categories are explained in more detail in Table 2.

Table 2

Impact Measurement Index Categories

IMI Category	Category Description
1	Any security incident that can be expected to cause serious damage to national security or DOE security interests.
2	Any security incident that can be expected to cause damage to national security or DOE security interests.
3	Any security incident with a low probability of causing damage to national security or DOE security interests.
4	Any security incident that causes no damage to national security, but that can, in combination, indicate weakened security awareness or inadequate procedures and practices.

Note: Descriptions in this table are taken verbatim from DoE N 471.3 (U.S. Department of Energy, 2001)

There is a fifth category of security events, not included in the IMI system, which was included in the present study. This category consists of those events that are determined to cause no damage to national security, and therefore do not fall into one of the four IMI categories. This type of event is often referred to as "sub-reportable"

because the occurrence of the event does not have to be reported to the DoE. However, sub-reportable events can be viewed as indicative of poor employee security behaviors because even though they do not result in damage to national security they occur as a result of employee actions or inactions which violate the established security protocols. This is somewhat analogous to the idea of near misses (Bird & Germain, 1996) or micro-accidents (Zohar, 2000) in the safety literature. Because they represent poor employee security behaviors, they were included in the current study.

Every security event in the Event data set had already been assigned a severity ranking, even if it was determined to be sub-reportable, by a trained investigator. Therefore, it was possible to create a metric of overall event severity that could be calculated for all divisions in both Year Two and Year Three. The metric was created by applying weights to the severity of the events that occurred in a given division over the course of a given year. The least severe of the five categories used in the study, sub-reportable events, was assigned a weight of 1. The second lowest category, IMI 4 events, was assigned a weight of 2. IMI 3 events were assigned a weight of 3, IMI 2 events were assigned a weight of 4, and the most severe IMI 1 events were assigned a weight of 5. Then each event in the data set was multiplied by the weight assigned to its level of severity. Finally, the weighted severity values for each of the events attributed to a division over the course of each year were added together and this sum was divided by the total number of security events attributed to the division over that same time period. This process was repeated for each division in both Year Two and Year Three. The result, essentially a weighted average of the severity of events occurring in a division over a one-year time period, served as the metric of event severity.

Division security exposure. Each division's security exposure, which refers to the amount of classified or sensitive work conducted within the division, was calculated based on data in the Exposure data set. The estimates of the percentage of classified work conducted by each division, provided by the five security experts, were averaged together to come up with an estimate that was not overly biased by any one individual's estimates. Prior to doing so, however, the estimates of all five of the experts were correlated to assess the reliability of these estimates. For Year Two, the correlations ranged from $r = .59$ to $r = .81$ and all were significant at the $p < .05$ level. For Year Three, the correlations ranged from $r = .59$ to $r = .82$ and again all were significant at the $p < .05$ level. Given these results, it was concluded that the expert's estimates were highly reliable. Therefore, the averages across all five experts were calculated for each division in both Year Two and Year Three and these averages were used as the metric of each division's security exposure.

Results

The results of this study are presented in three sections. First, evidence supporting the existence of the three distinct security climate dimensions proposed in Hypothesis 1a-1c are presented. Then, results supporting the emergent nature of security climate within divisions (proposed in Hypothesis 2a) and the relationship between security climate and security exposure (proposed in Hypothesis 2b) are presented. Finally, results of the analyses testing the relationship between security climate and various security performance metrics (proposed in H3a and H3b) are reported.

Dimensions of Security Climate

Hypothesis 1a-1c proposed that security climate is a multidimensional construct consisting of at least three separate dimensions including perceptions of management support for security (H1a), co-worker support for security (H1b), and security policies and procedures (H1c). The hypothesis was tested by analyzing the extent of agreement among judges in the sorting task. Since judges were instructed to group responses from the SME data set into categories representing the three proposed dimensions, results indication agreement in their sorting decisions would provide evidence supporting the construct validity of the three hypothesized dimensions.

Data from the sorting task was analyzed using a Microsoft Excel template (King, 2004) designed to calculate Fleiss's kappa (Fleiss, 1971). Fleiss's kappa, also referred to as generalized kappa, was chosen to assess agreement in this study because it was designed to assess the level of chance corrected agreement among judges using a nominal

or categorical response scale. In addition, unlike Cohen's kappa (Cohen, 1960) and weighted kappa (Cohen, 1968) which are restricted to situations where there are only two judges, Fleiss's kappa was designed for use where there are more than two judges as long as the number of judges rating each item or subject remains constant.

The agreement among judges (n = 6) sorting the 141 SME responses into the proposed categories (k = 4) was kappa = 0.68 ($p < .05$), 95% CI (0.65, 0.71). This finding is important because it suggests that agreement among judges' was significantly greater than what would be expected by chance. However, the calculation of kappa accounts for all sorting decisions across each category and therefore should only be interpreted as a measure of overall agreement among judges. In order to fully test the first hypothesis, agreement among judges within individual categories also had to be evaluated. Fortunately, it is possible to calculate kappa for individual categories using two equations provided by Fleiss (Equation 23 and Equation 27 in Fleiss, 1960).

Based on these equations, additional analyses were conducted to evaluate the agreement among judges within each of the three categories representing the proposed climate dimensions. Rater agreement for category one, the dimension of management support for security, was kappa = 0.85 ($p < .05$), 95% CI (0.72, 0.98). Thus Hypothesis 1a, which proposed that perceptions of management support for security is a dimension of security climate, was supported. Rater agreement for category two, the dimension of perceptions of co-worker support for security, was kappa = 0.63 ($p < .05$), 95% CI (0.51, 0.74). Thus Hypothesis 1b, which proposed that perceptions of co-worker support for security is a dimension of security climate, was supported. Rater agreement for category three, the dimension of security policies and procedures, was kappa = 0.68 ($p < .05$), 95%

CI (0.55, 0.82). Thus Hypothesis 1c, which proposed that perceptions of security policies and procedures are a dimension of security climate, was also supported.

Emergence of Security Climate

The second goal of this research was to determine whether a definable security climate does emerge within an organization and its sub-units, in this case divisions. Specifically, H2a proposed that security climate would be shared among employees working within the same division. In addition, H2a proposed that security climate would vary between divisions in relation to division security exposure. However, before these hypotheses could be tested, preliminary analyses were necessary to identify a subset of items from the organization's annual employee opinion survey that could serve as a measure of security climate.

Preliminary analyses. The process of identifying this subset of items (described above in the Measures section under the heading "Security Climate") led to the selection of just three items, out of fifty-two, that were deemed to assess dimensions of the security climate construct. These items included: 1) "My Supervisor is actively involved in promoting good security practices," 2) "I feel safe reporting potential security incidents in which I am directly involved," and 3) "I can readily obtain security information needed to perform my job." The first item was identified as a measure of the management support of security climate and the second and third items were both categorized as tapping the policies and procedures dimension of security climate. However, given the limited number of items overall, the limited number of items assigned to any single dimension, and the fact that the dimension of co-worker support for security was not represented by any items the decision was made to combine the three items into one

global security climate measure rather than grouping them into dimensional sub-scales. This approach also permitted a limited psychometric evaluation of the security climate measure.

The psychometric evaluation of the measure was conducted separately on data from Year One, Year Two, and Year Three. The first step was to analyze the proposed three-item security climate scale with confirmatory factor analysis via LISREL. The limited number of security climate items available in the data set made testing the single factor security measure problematic. Specifically, it constitutes a just-identified model and thus does not meet the statistical identification requirements inherent in structural equation modeling. In order to create a meaningful model that could be statistically evaluated, it was necessary to add two additional items to the proposed model. The additional items, drawn from the same employee opinion survey, assessed employees' perceptions of safety at the organization. By adding the safety items to the proposed model the issue of statistical identification was addressed. The additional items also created an opportunity to test the items' discriminant validity between the security climate and safety climate constructs.

The combination of the security and safety items resulted in a proposed two-factor measurement model consisting of three security items loading on a security climate factor and two safety items loading on a safety climate factor (see Figure 1). A one-factor competing model was also evaluated by constraining the correlation between the security and safety factors from the first model to be equal to 1.0. As a result, this one-factor model was nested within the two-factor model. Thus, the two models were contrasted based on the difference in χ^2 ($\Delta\chi^2$). A significant $\Delta\chi^2$ would provide evidence that the

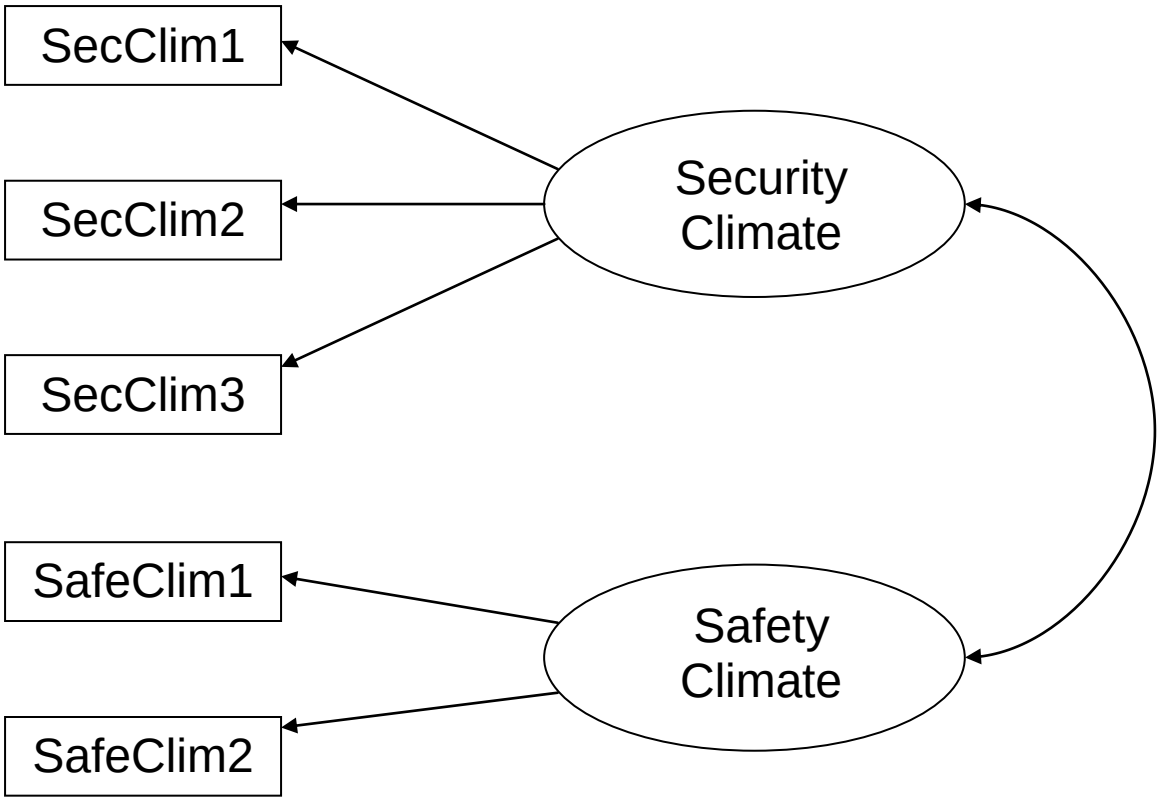

Figure 1. Two-factor measurement model for security climate and safety climate; one-factor model was derived by constraining the correlation between the two latent variables to 1.0.

proposed two-factor model fit the data better than the alternative one-factor model. The model comparison was repeated for each of the three years of climate data.

As shown in Table 3, the $\Delta\chi^2$ was significant in each of the three years. These results provide evidence of discriminant validity for the construct of security climate. And while the comparisons between the one-factor and two-factor models suggest that the two-factor model is superior on a relative basis, it was still necessary to establish the adequacy of the two-factor structure in and of itself. Therefore, results from the two-factor CFA (see Table 3) were reviewed in isolation to evaluate the fit of the proposed model.

The χ^2 statistic of overall fit was significant in Year One ($\chi^2(4) = 70.44$, $p < .05$), Year Two ($\chi^2(4) = 106.10$, $p < .05$) and Year Three ($\chi^2(4) = 85.78$, $p < .05$). These results suggest that the proposed two-factor model does not fit the data well. However a significant χ^2 is common when working with large sample sizes such as those from the three years of climate data that were analyzed here. To address this inherent problem with χ^2, a number of additional fit indices have been developed and were employed in the current study. The Normed Fit Index (NFI) represents the degree to which the model fits better than the baseline independence, or null, model and indicates the proportion of improvement in fit over a poorly fitting model (Bentler & Bonett, 1980). The NFI for Year One, Year Two, and Year Three were NFI = .99, NFI = .98, and NFI = .99 respectively indicating strong fit for the two-factor model in all three years. The Comparative Fit Index (CFI) is a revision of the NFI that was developed (Bentler, 1992) to take sample size into account. A CFI value of 0.95 or above indicates very good fit, but cutoff values having a magnitude of 0.90 or above are commonly viewed as

Table 3

Comparisons of the One-Factor and Two Factor Measurement Models

	χ^2	df	$\Delta\chi^2$	Δdf	NFI	CFI	GFI	AGFI	RMSEA
Year One									
Proposed Two-Factor Model	70.44*	4			.99	.99	.99	.97	.07
Alternative One-Factor Model	706.36*	5	635.92*	1	.90	.90	.93	.80	.17
Year Two									
Proposed Two-Factor Model	106.10*	4			.98	.99	.99	.95	.09
Alternative One-Factor Model	752.80*	5	646.70*	1	.89	.89	.93	.79	.18
Year Three									
Proposed Two-Factor Model	85.78*	4			.99	.99	.99	.96	.08
Alternative One-Factor Model	772.07*	5	686.29*	1	.89	.89	.93	.78	.18

*$p < .001$

Notes. NFI = normed fit index; CFI = comparative fit index; GFI = goodness of fit index; AGFI = adjusted goodness of fit index; RMSEA = root mean square error of approximation. Proposed model includes safety climate and security climate as separate factors. The alternative model combines safety and security into a single factor. $\Delta\chi^2$ and Δdf derived from model comparison.

acceptable (Bollen, 1989; Hoyle & Panter, 1995). The CFI indicated very good fit for Year One (CFI = .99), Year Two (CFI = .99), and Year Three (CFI = .99). The Goodness of Fit Index (GFI) evaluates the variance and covariance in the sample that is explained by a hypothesized population. Results from Year One (GFI = .99), Year Two (GFI = .99), and Year Three (GFI = .99) surpassed .90 which has been established as the cutoff for GFI values indicating good model fit. The Adjusted Goodness of Fit Index (AGFI) is identical to the GFI except that it is adjusted based on the degrees of freedom in the hypothesized model. AGFI results for Year One (AGFI = .97), Year Two (AGFI = .95), and Year Three (AGFI = .96) indicated good model fit for each year. The final fit statistic used was the RMSEA which is the root mean square error of approximation adjusted for degrees of freedom in the proposed model. Values of RMSEA that are greater than .10 are unacceptable (Steiger, 1990). In addition, Steiger has urged the reporting of 90% confidence intervals (CI) around the RMSEA value in order to determine the precision of these values (smaller confidence intervals indicate more precise estimates). The RMSEA results for Year One (RMSEA = .07; 90% CI = .055, .085), Year Two (RMSEA = .09; 90% CI = .074, .10) and Year Three (RMSEA = .08; 90% CI = .066, .095) were only modest. However, the RMSEA values were all below .10 and the 90% confidence intervals were relatively small and never exceeded .10. Therefore, these results were deemed acceptable indicators that the data fit the proposed model. Despite the significant χ^2 results, the unanimously positive results obtained for the subsequent fit indices suggests that the two-factor measurement model fits the data from all three years reasonably well.

Following the confirmatory factor analysis, item analyses were conducted to assess the reliability of the three item security climate measure. Item-total correlations and coefficient alpha were calculated for each of the three years. In Year One, item-total correlations ranged from $r = .44$ to $r = .48$ and coefficient alpha was .64. For Year Two, item-total correlations ranged from $r = .47$ to $r = .49$ and coefficient alpha was equal to .66. In Year Three, item-total correlations ranged from $r = .48$ to $r = .53$ while coefficient alpha was .68. These internal consistency results were deemed acceptable (although not ideal) given that the three items that comprise the scale address slightly different components of security climate. In light of the exploratory nature of the study, the decision was made to retain all three items for the security climate scale.

As a final analysis prior to testing H2a and H2b, the security climate data for each year were screened for the presence and pattern of missing data. Initially, Year One data contained 3694 cases distributed among 45 divisions (M = 82.09; SD = 86.53) and the response rate within each division ranged from 26% to 82% (M = 43%). After reviewing the data, 389 cases were deleted due to missing data. In addition, an a priori decision was made to exclude divisions with fewer than three cases and as a result three cases from two divisions were also deleted. This left 3302 cases and 43 divisions (M = 76.79; SD = 78.52). Two chi-square tests were conducted to explore the pattern of both response rates as well as missing data across divisions. The chi-square for response rates was found to be significant, $\chi^2(42) = 210.26$, $p < .05$. The result of the examination of missing data was also significant, $\chi^2(42) = 88.35$, $p < .05$. These findings suggest that divisions showed disproportional response rates and proportion of cases with missing data in Year One.

Year Two data contained 3711 cases distributed among 49 divisions (M = 75.73; SD = 76.27) and the response rate within each division, with the exception of one division where the population was unknown, ranged from 24% to 86% (M = 45%). After reviewing the data, 329 cases were deleted due to missing data and two cases from a single division were deleted because the division contained less than three cases. This left 3380 cases and 48 divisions (M = 70.42; SD = 70.13). As was done with Year One, the pattern of response rates and missing data were examined by way of chi-square tests. The result of the chi-square examining response rates was significant, $\chi^2(46) = 206.77$, $p < .05$. Likewise, the examination of missing data produced significant results, $\chi^2(47) = 82.75$, $p < .05$. This indicates that the rate of responding and the proportion of cases with missing data were unequal across divisions in Year Two.

Data from Year Three initially contained 3649 cases distributed among 53 divisions (M = 68.85; SD = 64.13) and the response rate within each division ranged from 26% to 83% (M = 44%). As a result of missing data, 325 cases were deleted. In addition, 2 cases were deleted because each was the sole response for their respective divisions, leaving 3322 cases and 51 divisions (M = 65.14; SD = 58.93). Again, the patterns of response rates and missing data were examined by way of two chi-square tests. The examination of response rates across divisions produced significant chi-square results, $\chi^2(50) = 279.18$, $p < .05$. A significant chi-square was also found when examining the proportion of missing cases across divisions, $\chi^2(50) = 101.76$, $p < .05$. As above, Year Three results suggest that divisions were unequal on both response rate as well as the proportion of cases with missing data.

Hypothesis 2a. In order to test the hypothesis that security climate perceptions are shared among employees working within the same division, and thus that it is an emergent phenomenon, the level of consensus among employees on the security climate measure was assessed. Consensus was assessed by calculating $r_{wg(j)}$ (James, Demaree, & Wolf, 1984, 1993), intraclass correlations (ICC1, Bartko, 1976; Shrout & Fleiss, 1979) where k was replaced by the harmonic mean of group size, the reliability of the mean (ICC2; Bartko, 1976), as well as between unit variance. These indices were calculated at the division level for all three years of data.

For Year One, the average $r_{wg(j)} = .76$ and ranged from .54 to .96. The intraclass correlation and reliability of the mean were found to be ICC1 = .08 and ICC2 = .59 respectively. Between unit variance was tested with one-way analysis of variance where respondents' division affiliation served as the independent variable and responses on the security climate scale was the dependent variable. Results indicated that the security climate was significantly different among divisions, $F(42, 3259) = 2.45$, $p < .05$.

Each of these indices were calculated for Year Two, resulting in an average $r_{wg(j)} = .74$ and ranged from .18 to .98. The intraclass correlation and reliability of the mean were ICC1 = .05 and ICC2 = .41 respectively. The one-way analysis of variance indicated that the security climate was significantly different among divisions, $F(47, 3332) = 1.70$, $p < .05$.

For Year Three, the average $r_{wg(j)} = .77$ and ranged from .32 to .98. The intraclass correlation and reliability of the mean were found to be ICC1 = .08 and ICC2 = .59 respectively. The one-way analysis of variance indicated that the security climate was significantly different among divisions, $F(50, 3271) = 2.41$, $p < .05$.

Taken together, the results obtained from data in Year One, Year Two, and Year Three support the assertion of Hypothesis 2a. That is, security climate perceptions do exhibit sufficiently high homogeneity among employees working within the same division so it can be said that the security climate construct is an emergent phenomenon. Therefore, individual responses were combined by averaging responses at the division level while testing each of the remaining hypotheses.

Hypothesis 2b. While the one-way analysis of variance results for Years One through Year Three described for H2a above suggest that security climate does vary among different divisions within the organization, Hypothesis 2b takes that idea one step further. Specifically, H2b proposes that divisions' security climate would be related to divisions' security exposure levels. To test this proposition, bivariate correlation coefficients were computed between each division's average security exposure ratings from the SME data set and the security climate measure aggregated at the division level. H2b was only tested using data from Year Two and Year Three because security exposure data was unavailable for Year One.

For Year Two, the correlation between security exposure and security climate was both negative and significant ($r = -.34$, $p < .05$, N = 48). The correlation for Year Three was also negative and significant ($r = -.29$, $p < .05$, N = 51). Taken together, these results provide support for Hypothesis 2b. Specifically, the significant negative correlations indicate that as security exposure increases security climate tends to decrease.

Outcomes of Security Climate

The third and final goal of the study was to explore whether security climate predicted security performance, over and above what is predicted by division security

exposure. To that end, Hypotheses 3a and 3b were proposed to examine the relationship between security climate, after controlling for division security exposure, and the security performance metrics of frequency of security incidents as well as severity of security events. These proposed relationships were tested with hierarchical regression. Specifically, for both security performance measures, four separate regression analyses were conducted. In each case, the first two analyses were structured to evaluate the effect of security climate on security performance immediately thereafter. For example, the security performance measure from Year Two served as the dependent variable while security exposure in Year Two (entered in the first step of the regression as a control) and security climate in Year Two (entered in the second step of the regression) served as the independent variables. This structure was then repeated using data from Year Three. The two remaining regression analyses were structured to evaluate the effect of security climate on security performance after a one year lag. For example, the security performance measure from Year Two served as the dependent variable while security exposure in Year Two (entered in the first step of the regression as a control) and security climate in Year One (entered in the second step of the regression) served as the independent variables. This analysis was then repeated with data from Year Two and Year Three.

As a final point, the rationale behind the structure of the last two analyses (using performance data from Year X in combination with climate data from Year X minus one) should be clear given the goal of exploring one year lagged effects. What might be less clear, and thus worthy of noting, is the rationale for using security exposure data from Year X rather than Year X minus one. Essentially, this decision had two key drivers.

First, we are interested in the lagged effects of security climate and not security exposure. Second, it seems reasonable to expect that security performance over the course of a year would be impacted by the security exposure (i.e. risk) that exists during that same time period rather than during the period before or after.

Preliminary analyses. Prior to conducting the regression analysis, a number of steps were taken to screen the data. First, every variable was examined for adherence to the assumptions of regression including normality as well as the existence of univariate and multivariate outliers. This screening process was repeated for each regression analysis. For this reason, as well as the presence of some missing data, sample sizes varied for each analysis.

Normality was assessed by exploring each variable for the presence of skewness or kurtosis. Examination of the two years of data collected for the two dependent variables (event frequency and event severity) did reveal evidence of non-normal distributions. Event frequency exhibited modest positive skew in Year Two and moderate positive skew and kurtosis in Year Three. Event severity data in Year Two showed evidence of modest positive skewness and kurtosis while Year Three showed signs of slight positive skewness but no kurtosis. Despite these results, the decision was made to forgo transforming the data to create normal distributions for two reasons. First, regression is typically robust to moderate violations, such as those found in the present study, of the normality assumption (Cohen, Cohen, West, & Aiken, 2003). In addition, data transformation is typically avoided if doing so makes it difficult to interpret results using data on a meaningful scale, which is the case for the two dependent variables. The independent variables were also examined for normality. Overall, all three years of

security climate data and both years of security exposure data were found to be normally distributed.

Variables were also examined for the presence of outliers. Univariate outliers were identified on the basis of cases 3.29 standard deviations above or below the mean and multivariate outliers were identified with Mahalanobis distance (using the generally accepted $p < .001$ level as the cutoff). Any cases identified as univariate or multivariate outliers were excluded from the analysis. Because the identification of multivariate outliers depends on the variables included in a given analysis, and there are a number of variable combinations employed in H3a and 3b, individual discussions of outliers will precede each of the regression analyses below.

In addition to the data screening just described, two steps were taken to conduct preliminary analysis of the data utilized in Hypothesis 3a and 3b prior to conducting the primary regression analyses. Descriptive statistics and correlations were calculated for all of the variables. These results, which are presented in Table 4, reveal a number of findings that merit attention. First, the near-perfect correlation between the security exposure ratings in Year Two and Year Three ($r = .99$, $p < .05$, N = 66) may be deemed suspect and perhaps the result of improper data entry. However, a review and reanalysis of the raw data led to the same result. Although it cannot be proven, a possible explanation for this extremely high correlation might be the way in which the data was collected. The yearly exposure data, consisting of average SME ratings of each division's exposure, were collected a little more than two years after the end of Year Three and both years of data were collected at the same time. It is possible that this led to error of measurement. Unfortunately, the process used to gather this information was the

Table 4

Descriptive Statistics and Correlations Among Hypothesis 3 Variables

	Mean	SD	1	2	3	4	5	6	7	8	9
1. Security Climate Year One	12.72	.74	--				.				
2. Security Climate Year Two	12.79	.75	.26	--							
3. Security Climate Year Three	12.77	.69	.68***	.56***	--						
4. Security Exposure Year Two	26.42	24.35	-.15	-.34*	-.28*	--					
5. Security Exposure Year Three	26.91	24.61	-.16	-.34*	-.29*	.99***	--				
6. Incident Frequency Year Two	5.16	5.88	.20	-.07	-.01	.54***	.53***	--			
7. Incident Frequency Year Three	4.83	9.56	.22	.02	.17	.08	.07	.22	--		
8. Incident Severity Year Two	1.93	.67	-.04	.38*	-.04	.03	.03	-.17	-.22	--	
9. Incident Severity Year Three	1.63	.50	-.10	-.04	-.08	.07	.07	-.30	-.29	.44**	--

* $p < .05$ ** $p < .01$ *** $p < .001$

N = 25 to 66

only method that was acceptable to the organization. However, as was mentioned previously, the interrater reliability among the SME ratings was sufficiently high to provide some confidence in the data that was collected.

Second, as the table indicates, the correlations between the three years of security climate data revealed that the correlation between Year One and Year Two was not significant ($r = .26$, $p > .05$, N = 39) whereas the correlations between Year One and Year Three as well as Year Two and Year Three were strongly positive ($r = .68$, $p < .05$, N = 34 and $r = .56$, $p < .05$, N = 42, respectively). These correlations could be interpreted as an assessment of test-retest reliability and the results suggest mixed evidence for the stability of the security climate measure over time. However, using these results to draw conclusions about the stability of the security climate measure may not be justified because it is not known whether the underlying variable being measured (security climate) should exhibit temporal stability. It has been argued that the general climate construct is difficult to alter once established (Ostroff et al., 2003), which implies stability over time. But research (e.g., Jackofsky & Slocum, 1988) has also shown that some types of climate (e.g., participative climate) are more stable than others (e.g., transcient climate). In light of these contrasting expectations regarding the stability of climate, the appropriateness of using the test-retest method to assess the reliability of the measure is unclear. Therefore, while acknowledging these mixed results, the conclusion of acceptable reliability of the security climate measure is maintained on the basis of these results and the internal consistency results discussed previously.

The last results from Table 4 that will be discussed are the correlations between frequency and severity of security events. The correlations between these two dependent

variables were not significant in either Year Two or Year Three, (r = -.17, p > .05, N = 38 and r = -.29, p > .05, N = 39, respectively). The non-significant correlations are important because they suggest that event frequency and event severity measure distinct aspects of a division's overall security performance. This can be viewed as support for their inclusion as two separate dependent variables in the current study.

One final set of preliminary analyses were conducted prior to running the main regression analyses meant to test Hypotheses 3a and 3b. This final step was deemed necessary due to the six significant chi-square results that were attained when exploring the pattern of response rates and proportion of cases with missing data from the security climate items. The significant chi-square results suggested that employee response rates to the survey as well as missing data within the three security climate items was disproportionate across the various divisions in each of the three years. This raised a legitimate question about whether the pattern of either response rates or missing data was in anyway related to the dependent variables utilized in H3a or H3b. If so, any possible relationships could potentially constitute a spurious relationship and thus call into question the robustness of the primary regression analyses if not controlled.

To examine this possibility the survey response rates and proportion of cases with missing data (which were both operationalized as percentages) from Year One, Year Two, and Year Three were correlated with the two dependent variables from Year Two and Year Three. The 24 correlations were calculated which ranged from r = -.27 to r = .23 and none were significant at the p < .01 level (which was used rather than .05 level used for the other analyses in this study to reduce the likelihood of Type 1 error). These results suggest that neither response rates nor missing data rates were likely to threaten

the planned regression analyses. Therefore, neither variable was controlled in the testing of Hypotheses 3a and 3b.

Hypothesis 3a. At this point it is now possible to focus attention on testing the proposed security climate – security performance relationships. I turn first to Hypothesis 3a which posited that security climate would predict the frequency of security events over and above what was predicted by security exposure. The first regression analysis conducted to test H3a included only data from Year Two. Exploration of Year Two data revealed two divisions with missing data which were therefore deleted. The data revealed no univariate or multivariate outliers. As a result, the final regression analysis was conducted on a total of 46 divisions.

To control for division security exposure, that variable was entered first into the regression equation and was found to be a significant predictor of security event frequency, $R^2 = .34$, $F(1,44) = 22.18$, $p < .05$. In the second step, security climate was entered into the regression equation. Results indicated that in Year Two security climate failed to predict security event frequency over and above security exposure, $\Delta R^2 = .03$, $F(1,43) = 2.19$, $p > .05$.

A second regression analysis, identical to the one above except that Year Three data was used in place of data from Year Two, was conducted to test H3a. None of the variables from Year Three contained missing data. One division was found to be a univariate outlier but no multivariate outliers were found. As a result, the final regression analysis was conducted on a total of 50 divisions.

Division security exposure was entered first into the regression equation and was found to be a significant predictor of event frequency, $R^2 = .11$, $F(1,48) = 5.71$, $p < .05$.

Security climate was then entered in the second step. Results indicated that in Year Three security climate was a significant predictor of security event frequency over and above security exposure $\Delta R^2 = .09$, $F(1,47) = 5.15$, $p < .05$.

In order to test for a lagged relationship between security climate and event frequency, a third regression analysis was conducted. Specifically, security event frequency from Year Two served as the dependent variable while security exposure from Year Two and security climate from Year One served as independent variables. None of the divisions contained either univariate or multivariate outliers. Due to the lack of Year One security climate data for a number of cases, only 39 divisions were included in the analysis.

Year Two security exposure was entered in the first step and was found to be a significant predictor of security event frequency in Year Two, $R^2 = .15$, $F(1,37) = 6.72$, $p < .05$. In the second step, security climate for Year One was entered. Results indicated that security climate for Year One was a significant predictor of event frequency in Year Two over and above Year Two security exposure, $\Delta R^2 = .10$, $F(1,36) = 4.93$, $p < .05$.

Finally, a fourth regression similar to the one above was completed to test for a lagged relationship between security climate and event frequency. In other words, security event frequency from Year Three served as the dependent variable and security exposure from Year Three and security climate from Year Two served as independent variables. No univariate or multivariate outliers were identified. Because of organizational restructuring between Year Two and Year Three, some divisions which existed in Year Two no longer existed in Year Three. Thus, those divisions were deleted listwise resulting in a total of 42 divisions that were included in the analysis.

After step 1, security exposure in Year Three was found to be a significant predictor of security event frequency in Year Three, $R^2 = .09$, $F(1,40) = 4.11$, $p < .05$. However, results from step 2 indicated that security climate for Year Two was not a significant predictor of event frequency in Year Three over and above Year Three security exposure, $\Delta R^2 = .02$, $F(1,39) = 0.61$, $p > .05$.

Overall, two of the four analyses found security climate significantly improved the prediction of event frequency over and above security exposure alone. However, a more detailed examination of the results (see Table 5) revealed positive regression weights (β) on security climate for both of the above significant results (i.e., security climate in Year 1 predicted security event frequency in Year 2, and security climate in Year 3 predicted security event frequency in Year 3). This suggests that as security climate increases so does event frequency, which runs counter to the proposed direction of the relationship. Therefore, it is impossible to claim even mixed support for Hypothesis 3a.

Nonetheless, these significant findings were further scrutinized in order to provide some clarity regarding the nature of the results. Additional review of the results revealed tolerance levels well within acceptable limits indicating no problems of multicollinearity in either analysis. However, evidence of a suppression effect was present in both sets of results. In brief, a suppressor variable is identified if its inclusion in a regression equation improves the predictive validity of a second variable simply by suppressing criterion-irrelevant variance from the second variable. The classical notion of suppression (Horst, 1941) has been expanded to include additional situations such as negative suppression (Darlington, 1968) and reciprocal suppression (Conger, 1974). The

Table 5

Summary of Hierarchical Regression for Variables Predicting Security Event Frequency

	Year Two[a]		Year Three[b]		One Year Lag – Y1 to Y2[c]		One Year Lag – Y2 to Y3[d]	
	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2
Security Exposure (β)	.58***	.64***	.33*	.41**	.39*	.44**	.31*	.34*
Security Climate (β)		.19		.31*		.32*		.12
R^2	.34***	.37***	.11*	.20**	.15*	.26**	.09*	.11
ΔR^2		.03		.09*		.10*		.02
Adjusted R^2	.32***	.33***	.09*	.16**	.13*	.21**	.07*	.06

[a] Analysis using frequency data from Year Two, exposure data from Year Two, and security climate data from Year Two; N = 46

[b] Analysis using frequency data from Year Three, exposure data from Year Three, and security climate data from Year Three; N = 50

[c] Analysis using frequency data from Year Two, exposure data from Year Two, and security climate data from Year One; N = 39

[d] Analysis using frequency data from Year Three, exposure data from Year Three, and security climate data from Year Two; N = 42

* $p < .05$, ** $p < .01$, *** $p < .001$

focus here will be on the later situation, reciprocal suppression, because the pattern of results point to the occurrence of this type of suppression.

Reciprocal suppression in a two-predictor regression equation occurs when each predictor variable is acting as a suppressor on the other. The existence of reciprocal suppression can be identified when two predictors are positively correlated with a criterion, are negatively correlated with each other, and both predictors' zero-order correlations with the criterion are smaller than their respective βs. All of these conditions were present in the results of both significant analyses from H3a which suggests the existence of reciprocal suppression effects. Because this pattern was found in some of the remaining analyses, results for each will be summarized prior to the discussion of how to interpret regression findings when suppression occurs.

Hypothesis 3b. Hypothesis 3b proposed that security climate would predict severity of security events over and above what was predicted by security exposure. Following the process used for H3a, the proposed relationship in H3b was tested via four separate regression analyses. The first and second analyses used data from Year Two and data from Year Three, respectively. These were then followed by two additional lagged analyses, first using combined data from Years One and Two and then using combined data from Years Two and Three.

Exploration of data from Year Two revealed a number of divisions that contained missing data. This was because average event severity could not be calculated for divisions that did not experience any security events in Year Two. However, no univariate or multivariate outliers were identified. As a result, the final regression analysis was conducted on a total of 38 divisions.

Severity of security events served as the dependent variable in the regression equation. As before, in order to control for division security exposure it was entered in the first step of the regression equation. Results indicated that security exposure in Year Two was not a significant predictor of event severity in Year Two, $R^2 = .00$, $F(1,36) = 0.01$, $p > .05$. Then Year Two security climate was entered in the second step of the regression and was found to be a significant predictor of event severity over and above security exposure $\Delta R^2 = .15$, $F(1,35) = 6.01$, $p < .05$.

A second regression analysis, identical to the one above except that Year Three data was used in place of data from Year Two, was conducted to test H3b. Exploration of data from Year Three, as with Year Two, revealed a number of cases with missing data due to the inability to calculate event severity for divisions that experienced no security events. Again, no univariate or multivariate outliers were found. As a result, the final regression analysis was conducted on a total of 39 divisions.

The regression was conducted by entering security exposure into the first step and security climate in the second step. Results from the first step of the regression equation indicated that in Year Three security exposure was not a significant predictor of security event severity, $R^2 = .01$, $F(1,37) = 0.19$, $p > .05$. Results from step 2 of the analysis indicated that in Year Three security climate was not a significant predictor of event severity over and above security exposure $\Delta R^2 = .01$, $F(1,36) = 0.14$, $p > .05$.

In order to test for a lagged relationship between security climate and event severity, severity of security events from Year Two served as the dependent variable while security exposure from Year Two and security climate from Year One served as independent variables. Exploration of the data revealed no univariate or multivariate

outliers. But as before, a number of cases lacked security climate events in Year Two so event severity could no be calculated. In addition, a number of divisions in Year One lacked security climate data. As a result, only 31 divisions were included in the analysis.

Year Two security exposure was entered in the first step of the regression but was not found to be a significant predictor event severity in Year Two, $R^2 = .01$, $F(1,29) = 0.14$, $p > .05$. Likewise, the results from step 2 found that security climate in Year One did not significantly add to the prediction of event severity in Year Two over and above Year Two security exposure, $\Delta R^2 = .01$, $F(1,28) = 0.03$, $p > .05$.

Finally, a fourth regression similar to the one above was completed. Severity of security events from Year Three served as the dependent variable and security exposure from Year Three and security climate from Year Two served as independent variables in order to test for a lagged relationship between security climate and event severity. No univariate or multivariate outliers were identified. However, event severity could not be calculated for some divisions and thus those cases were excluded from the analysis due to missing data. As a result, a total of 33 divisions were included in the analysis. Results from step 1 indicated that Year Three security exposure was not a significant predictor event severity in Year Three, $R^2 = .01$, $F(1,31) = 0.18$, $p > .05$. Likewise, the results from step 2 found that security climate for Year Two was not a significant predictor of event severity in Year Three over and above Year Three security exposure, $\Delta R^2 = .01$, $F(1,30) = 0.03$, $p > .05$.

In summary, only one of the four regression analyses showed security climate to significantly predict event severity beyond security exposure. Unfortunately, as with the results from H3a, the results from the one significant analysis show that the β for security

climate is positive (see Table 6). This suggests that as security climate increases so does the severity of security events, which is opposite of the proposed relationship. However, the presence of reciprocal suppression was again identified.

Supplemental analyses. Given the exploratory nature of this study, the decision was made to conduct additional supplemental analyses in order to attempt to shed further light on the security climate-security performance relationship. The first two sets of supplemental analyses sought to further explore the security climate – event frequency relationship proposed in H3a by breaking the original dependent variable of event frequency into two separate frequency metrics. Specifically, measures of frequency of self-reported events (those events that were reported to the organization by one or more of the individuals responsible for the event) and frequency of non-self-reported events (those events discovered by the organization in a way other than self-reporting) were created. In both cases, these frequency metrics were standardized on the basis of division size using the same process used to standardize overall event frequency.

The second two sets of supplemental analyses sought to further explore the security climate – event severity relationship proposed in H3b. To do this, two new dependent variables were created. The first, frequency of reportable events, was calculated by grouping and tallying all of the reportable (i.e. IMI1-IMI4) events in a division and standardizing based on division size. The second, frequency of sub-reportable events, consisted of a tally of each division's sub-reportable events and again standardizing the totals based on division size.

Using these four new dependent variables, four sets of four regression analyses were run using the same pattern employed to test H3a and H3b. Results from the

Table 6

Summary of Hierarchical Regression for Variables Predicting Security Event Severity

	Year Two[a]		Year Three[b]		One Year Lag – Y1 to Y2[c]		One Year Lag – Y2 to Y3[d]	
	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2
Security Exposure (β)	-.01	.04	.07	.06	.07	.06	.08	.07
Security Climate (β)		.39*		-.06		-.03		-.03
R^2	.00	.15	.00	.01	.00	.01	.00	.01
ΔR^2		.15*		.01		.01		.01
Adjusted R^2	-.03	.10	-.02	-.05	-.03	-.07	-.03	-.06

[a] Analysis using severity data from Year Two, exposure data from Year Two, and security climate data from Year Two; N = 38

[b] Analysis using severity data from Year Three, exposure data from Year Three, and security climate data from Year Three; N = 39

[c] Analysis using severity data from Year Two, exposure data from Year Two, and security climate data from Year One; N = 31

[d] Analysis using severity data from Year Three, exposure data from Year Three, and security climate data from Year Two; N = 33

* $p < .05$, ** $p < .01$, *** $p < .001$

supplemental analyses using the dependent variable of frequency of self-reporting events (hereafter, simply self-reporting) are discussed first. This will be followed by discussion of results using frequency of non-self-reporting events (non-self-reporting), followed by frequency of reportable events (reportable events), and finally frequency of sub-reportable events (sub-reportable events).

The first regression analysis conducted to explore the security climate – self-reporting relationship included only data from Year Two. Exploration of these variables for missing data, univariate outliers, and multivariate outliers resulted in regression analysis with a total of 46 divisions. In order to control for division security exposure, that variable was entered first into the regression equation and was found to be a significant predictor of self-reporting, $R^2 = .36$, $F(1,44) = 24.98$, $p < .05$. In the second step, security climate was entered into the regression equation. Results indicated that in Year Two security climate failed to predict self-reporting over and above security exposure, $\Delta R^2 = .01$, $F(1,43) = 0.50$, $p > .05$.

A second regression analysis, identical to the one above except that Year Three data was used in place of data from Year Two, was then conducted. One case was deleted as a univariate outlier resulting in a regression analysis with a total of 50 divisions. Division security exposure was entered first into the regression equation and was found to be a significant predictor of self-reporting, $R^2 = .09$, $F(1,48) = 4.50$, $p < .05$. Security climate was then entered in the second step. Results indicated that in Year Three security climate was not a significant predictor of self-reporting over and above security exposure $\Delta R^2 = .06$, $F(1,47) = 3.27$, $p > .05$.

In order to test for a lagged relationship between security climate and self-reporting, a third regression analysis was conducted with a combination of data from Year One and Year Two. Self-reporting from Year Two served as the dependent variable while security exposure from Year Two and security climate from Year One served as independent variables. Due to the lack of Year One security climate data for a number of cases, only 39 divisions were included in the analysis. Year Two security exposure was entered in the first step and was found to be a significant predictor of self-reporting in Year Two, $R^2 = .23$, $F(1,37) = 10.99$, $p < .05$. In the second step, security climate for Year One was entered. Results indicated that security climate for Year One was not a significant predictor of self-reporting in Year Two over and above Year Two security exposure, $\Delta R^2 = .01$, $F(1,36) = 0.17$, $p > .05$.

A fourth and final regression similar to the one above was completed using data from Year Two and Year Three. Because of organizational restructuring between Year Two and Year Three, a total of 42 divisions were included in the analysis. After step 1, security exposure in Year Three was found to not be a significant predictor self-reporting in Year Three, $R^2 = .09$, $F(1,40) = 3.91$, $p > .05$. In addition, results from step 2 indicated that security climate for Year Two was not a significant predictor of self-reporting in Year Three over and above Year Three security exposure, $\Delta R^2 = .04$, $F(1,39) = 1.72$, $p > .05$.

When reviewing the results from the four regression analyses (see Table 7), there was no support for a relationship between security climate and self-reporting. Specifically, none of the regression analyses found security climate to be a significant

Table 7

Summary of Hierarchical Regression for Variables Predicting Frequency of Self-Reported Events

	Year Two[a]		Year Three[b]		One Year Lag – Y1 to Y2[c]		One Year Lag – Y2 to Y3[d]	
	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2
Security Exposure (β)	.60***	.63***	.29*	.36*	.48**	.49**	.30	.24
Security Climate (β)		.09		.25		.06		-.21
R^2	.36***	.37***	.09*	.15*	.23**	.24**	.09	.13
ΔR^2		.01		.06		.01		.04
Adjusted R^2	.35***	.37***	.07*	.11*	.21**	.10**	.07	.08

[a] Analysis using self-report data from Year Two, exposure data from Year Two, and security climate data from Year Two; N = 46

[b] Analysis using self-report data from Year Three, exposure data from Year Three, and security climate data from Year Three; N = 50

[c] Analysis using self-report data from Year Two, exposure data from Year Two, and security climate data from Year One; N = 39

[d] Analysis using self-report data from Year Three, exposure data from Year Three, and security climate data from Year Two; N = 42

* $p < .05$, ** $p < .01$, *** $p < .001$

predictor of self-reporting over and above security exposure. However, results from Year Three and the second one-year lag did approach significance.

The supplemental analyses exploring the relationship between security climate and non-self-reporting began with a regression using data from Year Two. After deletion of two cases found to be univariate outliers, the final regression analysis was conducted on a total of 45 divisions. In order to control for division security exposure, that variable was entered first into the regression equation and was found to be a significant predictor of non-self-reporting, $R^2 = .25$, $F(1,43) = 14.14$, $p < .05$. In the second step, security climate was entered into the regression equation. Results indicated that in Year Two security climate did predict non-self-reporting over and above security exposure, $\Delta R^2 = .09$, $F(1,42) = 5.88$, $p < .05$.

A second regression analysis, identical to the one above except that Year Three data was then run. After deleting cases found to be univariate outliers, a total of 49 cases were included in the analysis. Division security exposure was entered first into the regression equation and was found to be a significant predictor of non-self-reporting, $R^2 = .10$, $F(1,47) = 5.40$, $p < .05$. Security climate was then entered in the second step. Results indicated that in Year Three security climate was not a significant predictor of non-self-reporting over and above security exposure $\Delta R^2 = .02$, $F(1,46) = 0.5$, $p > .05$.

To test for a lagged relationship between security climate and event frequency, a third regression analysis was conducted using a combination of data from Year One and Year Two. Non-self-reporting from Year Two served as the dependent variable while security exposure from Year Two and security climate from Year One served as independent variables. Due to the lack of Year One security climate data for a number of

cases, as well as the existence of two cases found to be univariate outliers, only 37 divisions were included in the analysis.

Year Two security exposure was entered in the first step and was found to be a significant predictor non-self-reporting in Year Two, $R^2 = .21$, $F(1,35) = 9.15$, $p < .05$. In the second step, security climate for Year One was entered. Results indicated that security climate for Year One was a significant predictor of non-self-reporting in Year Two over and above Year Two security exposure, $\Delta R^2 = .14$, $F(1,34) = 7.18$, $p < .05$.

Finally, a fourth regression similar to the one above was completed to again test for a lagged relationship between security climate and non-self-reporting. Data from Year Two and Year Three were combined such that non-self-reporting from Year Three served as the dependent variable and security exposure from Year Three and security climate from Year Two served as independent variables. Because of organizational restructuring between Year Two and Year Three, some divisions which existed in Year Two no longer existed in Year Three. Thus those divisions were deleted listwise due to missing data. In addition, one case was deleted because it was found to be a univariate outlier. As a result, a total of 41 divisions were included in the analysis. After step 1, security exposure in Year Three was found to be a significant predictor non-self-reporting in Year Three, $R^2 = .11$, $F(1,39) = 4.93$, $p < .05$. In addition, results from step 2 indicated that security climate for Year Two was a significant predictor of non-self-reporting in Year Three over and above Year Three security exposure, $\Delta R^2 = .18$, $F(1,38) = 9.48$, $p < .05$.

Three of the four analyses found security climate to be a significant predictor of non-self-reporting behavior over and above security exposure. However, these results are

once again revealed to be problematic when reviewing Table 8. While no relationship between climate and non-self-reporting was formally hypothesized, logic would suggest that the relationship would be negative because the organization requires employees to self-report security incidents that they are involved in. Therefore, failing to do so essentially constitutes a violation of security procedure in addition to the original actions that caused the event. But the security climate βs were again positive which suggests that as security climate increases so does non-self-reporting. As before, presence of reciprocal suppression was detected in the results of all three significant analyses.

The supplemental analysis conducted to explore the relationship between security climate and reportable events began by running a regression analysis employing data from Year Two. One case was deleted due to missing data and as a result the final regression analysis was conducted on a total of 47 divisions.

In order to control for division security exposure, that variable was entered first into the regression equation. The results indicated that security exposure in Year Two was a significant predictor of reportable events, $R^2 = .12$, $F(1,45) = 6.20$, $p < .05$. In the second step, security climate was entered into the regression equation. Results indicated that in Year Two security climate failed to predict reportable events over and above security exposure, $\Delta R^2 = .04$, $F(1,44) = 2.07$, $p > .05$.

A second regression analysis was then run using data from Year Three. One case was deleted after it was found to be a univariate outlier. As a result, the final regression analysis was conducted on a total of 50 divisions. Division security exposure was entered first into the regression equation. Results indicated that it was a significant predictor of reportable events, $R^2 = .16$, $F(1,48) = 9.05$, $p < .05$. Security climate was

Table 8

Summary of Hierarchical Regression for Variables Predicting Frequency of Non-Self-Reported Events

	Year Two[a]		Year Three[b]		One Year Lag – Y1 to Y2[c]		One Year Lag – Y2 to Y3[d]	
	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2
Security Exposure (β)	.50***	.60***	.32*	.37*	.46**	.51***	.34*	.45**
Security Climate (β)		.32*		.14		.38*		.44**
R^2	.25***	.34***	.10*	.12	.21**	.35***	.11*	.29**
ΔR^2		.09*		.02		.14*		.18**
Adjusted R^2	.23***	.31***	.08*	.08	.19**	.31***	.09*	.25**

[a] Analysis using non-self-report data from Year Two, exposure data from Year Two, and climate data from Year Two; N = 45

[b] Analysis using non-self-report data from Year Three, exposure data from Year Three, and climate data from Year Three; N = 49

[c] Analysis using non-self-report data from Year Two, exposure data from Year Two, and climate data from Year One; N = 37

[d] Analysis using non-self-report data from Year Three, exposure data from Year Three, and climate data from Year Two; N = 41

* $p < .05$, ** $p < .01$, *** $p < .001$

then entered in the second step but the results suggested that it was not a significant predictor of reportable events over and above security exposure $\Delta R^2 = .02$, $F(1,47) = 1.17$, $p > .05$.

In order to test for a lagged relationship between security climate and reportable events, reportable events from Year Two served as the dependent variable while security exposure from Year Two and security climate from Year One served as independent variables. Due to the lack of security climate data for Year One cases, only 39 divisions were included in the analysis. Year Two security exposure was entered in the first step but was not found to be a significant predictor of reportable events in Year Two, $R^2 = .04$, $F(1,37) = 1.51$, $p > .05$. In the second step, security climate for Year One was entered. Results indicated that security climate for Year One was not a significant predictor of reportable events in Year Two over and above Year Two security exposure, $\Delta R^2 = .03$, $F(1,36) = 1.05$, $p > .05$.

Finally, a fourth regression similar to the one above was completed using a combination of data from Year Two and Year Three. Because of organizational restructuring between Year Two and Year Three, some divisions which existed in Year Two no longer existed in Year Three. Thus those divisions, along with one case found to be a univariate outlier, were deleted. As a result, a total of 41 divisions were included in the analysis. After step 1, security exposure in Year Three was found to be a significant predictor of reportable events in Year Three, $R^2 = .14$, $F(1,39) = 6.30$, $p < .05$. However, results from step 2 indicated that security climate for Year Two was not a significant predictor of reportable events in Year Three over and above Year Three security exposure, $\Delta R^2 = .08$, $F(1,38) = 3.77$, $p > .05$.

The results from these four regression analyses (see Table 9), provide no support for a relationship between security climate and reportable events. None of the analyses found security climate to be a significant predictor of reportable events over and above what was predicted by security exposure. However, results from the second lagged analysis did approach significant ($p = .06$) and the β was in the expected direction.

The final set of supplemental analyses was meant to explore any potential relationship between security climate and sub-reportable events. Exploration of data from Year Two revealed one division with missing data which was excluded. This left a total of 47 cases for inclusion in the regression analysis Similar to the previous analyses, division security exposure was entered in the first step of the regression equation and was found to be a significant predictor of sub-reportable events, $R^2 = .33$, $F(1,45) = 21.89$, $p < .05$. When entered in the second step, security climate was found to not be a significant predictor of sub-reportable events over and above security exposure in Year Two, $\Delta R^2 = .00$, $F(1,44) = 0.03$, $p > .05$.

The above process was repeated for data from Year Three. Exploration of data from Year Three found one division to be a univariate outlier and it was deleted. As a result, the final regression analysis was conducted on a total of 50 divisions. As was the case above, division security exposure entered in the first step was determined to be a significant predictor of sub-reportable events, $R^2 = .09$, $F(1,48) = 4.78$, $p < .05$. Likewise, results from the second step of the analysis indicated that security climate for Year Three was a significant predictor of sub-reportable events over and above security exposure, $\Delta R^2 = .09$, $F(1,47) = 5.06$, $p < .05$.

Table 9

Summary of Hierarchical Regression for Variables Predicting Frequency of Reportable Events

	Year Two[a]		Year Three[b]		One Year Lag – Y1 to Y2[c]		One Year Lag – Y2 to Y3[d]	
	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2
Security Exposure (β)	.35*	.41**	.40**	.44**	.20	.22	.37*	.30
Security Climate (β)		.21		.15		.17		-.29
R^2	.12*	.16*	.16**	.18**	.04	.07	.14*	.22**
ΔR^2		.04		.02		.03		.08
Adjusted R^2	.10*	.12*	.14**	.14**	.01	.01	.12*	.18**

[a] Analysis using reportable data from Year Two, exposure data from Year Two, and climate data from Year Two; N = 47

[b] Analysis using reportable data from Year Three, exposure data from Year Three, and climate data from Year Three; N = 50

[c] Analysis using reportable data from Year Two, exposure data from Year Two, and climate data from Year One; N = 39

[d] Analysis using reportable data from Year Three, exposure data from Year Three, and climate data from Year Two; N = 41

* $p < .05$, ** $p < .01$, *** $p < .001$

In order to test for a lagged relationship between security climate and sub-reportable events, a third regression analysis was conducted. Sub-reportable events from Year Two served as the dependent variable while security exposure from Year Two and security climate from Year One served as independent variables. None of the divisions contained variables that could be identified as either univariate or multivariate outliers. However, the lack of Year One security climate data resulted in sample size of only 39 divisions for this analysis. Year Two security exposure was entered in the first step and was a significant predictor of sub-reportable events in Year Two, $R^2 = .20$, $F(1,37) = 9.35$, $p < .05$. Security climate for Year One was then entered in the second step. Results indicated that security climate for Year One significantly added to the prediction of sub-reportable events in Year Two over and above Year Two security exposure, $\Delta R^2 = .13$, $F(1,36) = 7.06$, $p < .05$.

Finally, a fourth regression similar to the one above was completed to again test for a lagged relationship between security climate and sub-reportable events. Sub-reportable events from Year Three served as the dependent variable and security exposure from Year Three and security climate from Year Two served as independent variables. No univariate or multivariate outliers were identified. As before, some divisions which existed in Year Two no longer existed in Year Three. As a result, a total of 42 divisions were included in the analysis. Security exposure from Year Three was entered into the first step of the regression and the results indicated that it was a significant predictor of sub-reportable events in Year Three, $R^2 = .09$, $F(1,40) = 4.09$, $p < .05$. Security climate for Year Two was then entered in the second step and was found

not to be a significant predictor of sub-reportable events in Year Three over and above Year Three security exposure, $\Delta R^2 = .03$, $F(1,39) = 1.24$, $p > .05$.

While two of the four analyses were significant, the results must once again be interpreted within the context of findings shown in Table 10 on the next page. In both cases the β for security climate was positive which is opposite of what might be logically assumed. And as before, reciprocal suppression was identified in both sets of results.

Ultimately a lack of consistent significant results, and the presence of reciprocal suppression whenever significance was found, in both the hypothesized and supplemental analyses make it impossible to suggest support for a security climate – security performance relationship in the proposed form. However, an alternative way to utilize these results will be addressed in the discussion section which follows.

Table 10

Summary of Hierarchical Regression for Variables Predicting Frequency of Sub-Reportable Events

	Year Two[a]		Year Three[b]		One Year Lag – Y1 to Y2[c]		One Year Lag – Y2 to Y3[d]	
	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2	Step 1	Step 2
Security Exposure (β)	.57***	.57***	.30*	.39**	.45**	.50***	.30*	.36*
Security Climate (β)		-.02		.31*		.37*		.18
R^2	.33***	.33***	.09*	.18**	.20**	.33***	.09*	.12
ΔR^2		.00		.09*		.13*		.03
Adjusted R^2	.31***	.30***	.07*	.14**	.18**	.30***	.07*	.08

[a] Analysis using sub-reportable data from Year Two, exposure data from Year Two, and climate data from Year Two; N = 47

[b] Analysis using sub-reportable data from Year Three, exposure data from Year Three, and climate data from Year Three; N = 50

[c] Analysis using sub-reportable data from Year Two, exposure data from Year Two, and climate data from Year One; N = 39

[d] Analysis using sub-reportable data from Year Three, exposure data from Year Three, and climate data from Year Two; N = 42

* $p < .05$, ** $p < .01$, *** $p < .001$

Discussion

Experts in the field of security have begun contemplating organizational characteristics such as climate and culture as potential factors that may contribute to security events within organizations. Despite this interest, these ideas have received very little follow-up in the form of empirical research. In light of the limited amount of work on the topic, the current study sought to conduct an exploratory investigation of security climate. To do so, a number of steps were completed.

First, a conceptualization of the security climate construct had to be developed. To that end, relevant literature from fields related to security was reviewed in order to identify potential dimensions of security climate. This literature review lead directly to Hypotheses 1a-1c which proposed three separate dimensions of security climate. The analyses provided support for the validity of all three dimensions. The study then sought to confirm the emergent nature of the construct in order to establish that security climate was definable at the unit level of measurement. For that reason, Hypothesis 2a proposed that security climate would be shared at the division level and Hypothesis 2b proposed that division security climate would be related to division security exposure. Both H2a and H2b were supported, which suggests that security climate is an emergent phenomenon. The final aim of the study was to determine what impact, if any, security climate has on security performance. Therefore, Hypotheses 3a and 3b were put forth positing that security climate would be negatively related to frequency of security events and severity of security events, respectively. Analyses revealed the presence of

reciprocal suppression, so no conclusions could be drawn regarding the climate-performance relationships proposed in H3a and H3b. However, an examination of zero order correlations did reveal a few significant relationships between security climate and the various security performance metrics. But these significant findings were limited and not in the predicted direction.

A brief review of all the results from the study, as well as a more in depth discussion of conclusions drawn in that context, are presented in the first three sections. Then the theoretical and practical implications of the study findings are examined. Thereafter, limitations of the study and directions for future research are discussed. The last section concludes with a few final thoughts regarding the study as a whole.

Development of Climate for Security

In order to investigate the concept of security climate, the construct had to be operationalized in a meaningful way. As such, three security climate dimensions were proposed in Hypotheses 1a-1c, all of which were supported by the results from the sorting task. These findings allow for a number of important conclusions regarding the structure of security climate.

First, the findings suggest that security climate can be viewed as multi-dimensional. This conclusion is important because it is in line with the traditional view that organizational climate is a multi-dimensional construct (e.g., Campbell et al., 1970). Without question, this alone does not prove the existence of security climate. However, if a multi-dimensional structure was not supported, one possible interpretation of the findings might have been that the construct being investigated was not a type of climate.

While evidence of the multi-dimensional nature of the construct is important, the findings allow for a more specific – and practical – conclusion regarding security climate. Specifically, support for Hypotheses 1a-1c make it possible to conclude that security climate can be operationally defined as employees' perceptions of management support for security (H1a), co-worker support for security (H1b), and security policies and procedures (H1c). The importance of this conclusion for the conceptual development of security climate cannot be overstated. Establishing a sound operational definition is critical because security climate is an example of a psychological construct (also known as a psychological attribute or psychological trait); which means it is a theoretical concept that cannot be directly observed or measured. In fact, the existence of any psychological construct (including personality characteristics, emotions, and organizational climate) can only be deduced indirectly by quantifying observable phenomena, known as manifest variables, which are thought to occur as a result of some hypothesized psychological construct. In theory, measuring one or more manifest variables (such as physical characteristics, physiological responses, or specific behaviors) displayed by a subject can be used to gauge the level of a psychological construct present in that subject. However, this idea is only tenable if there is a real relationship between the existence of a psychological construct and the occurrence of a manifest variable. And while no assessment of a manifest variable will ever be a perfect proxy for the assessment of a psychological construct, a good operational definition can help to increase the congruence between the two.

As an example, consider research similar to the current study which employs survey methodology to investigate a psychological construct. When using survey

techniques, each item can be viewed as a stimulus and each item response can be viewed as a discrete sample of behavior that can serve as a manifest variable. In this context, the level of congruence between the psychological construct and a particular manifest variable is dependent on the stimulus item that elicited the observed behavior. If the item taps content that is relevant to the psychological construct, the resulting manifest variable will have a high level of congruence with the construct. If the item addresses content that is not relevant to the psychological construct, congruence between the manifest variable and the construct will be low. The importance of a good operational definition is that it specifically outlines the content area believed to be relevant to the psychological construct. This information can then be used to create items which will elicit manifest variables that are congruent with the psychological construct. As a result of this congruence, the manifest variables (i.e., the item responses) can serve as an indirect measure of the psychological construct.

As has been discussed, the current study relied on archival data so the development of new items was not possible. However, the operational definition of security climate was used to select existing items for inclusion in the security climate measure. While the resulting scale did have shortcomings (only three items were selected and only two of the three proposed dimensions were represented by those items), the item selection process did produce a measure with a stable factor structure which demonstrates evidence of reliability as well as discriminant validity (Campbell & Fiske, 1959). These findings provided support for using the measure to address the two remaining goals of the study, testing the emergent nature of security climate and investigating possible antecedents of the concept.

Emergence of Security Climate

The second goal of the study was to determine if security climate is an emergent phenomenon, meaning that it "originates in the cognition, affect, behaviors or other characteristics of individuals, is amplified by their interaction, and manifests as a higher level, collective phenomenon" (Kozlowski & Klein, 2000, p. 55). In other words, security climate can be called an emergent phenomenon if perceptions regarding security are shared at the group level. To that end, H2a proposed that shared perceptions regarding security would exist within divisions (which served as the group level of measurement in this study). Using individuals' responses on the security climate measure, three separate indices of consensus (r_{wg}, ICC1, and ICC2) were calculated to assess the extent of agreement among employees within the same division. In addition, a one-way analysis of variance was calculated to determine if security perceptions would differ among divisions.

Results from these analyses, which were repeated for each of the three years of available data, support the assertion of Hypothesis 2a that individual employees' perceptions regarding security tend to be shared by others within the same division. Therefore, it is possible to conclude that security climate is an emergent phenomenon. In addition, the ANOVA results suggest that perceptions of security varied among divisions. Because shared perceptions of security exist at the division level and these shared perceptions differ among divisions, the findings suggest that security climate may emerge at the division level of the organization. However, these results do not explain why the emergence of security climate occurs at the division level.

According to Zohar (2000), if climate exists at the group level then sources of climate perceptions should also be at the group level. With that in mind, Hypothesis 2b posited that the security climate within a division would be related to the security exposure of that division. The hypothesis was supported by significant negative correlations between division security climate and division security exposure. These results indicate that higher (i.e. more positive) security climate tends to emerge in divisions with low security exposure and lower (i.e. more negative) security climate tends to emerge in divisions with high security exposure.

These findings are important to the goals of this study for a number of reasons. First of all, the results suggest that a portion of the divisional differences in security climate can be explained by the variance in division security exposure. In addition, it has been argued (e.g., Crocker & Algina, 1986) that the development of novel psychological constructs such as security climate must go beyond the establishment of an operational definition by evaluating the construct through quantitative comparisons with other similar variables. Correlating division security climate with division security exposure in the current study was a first attempt at such an evaluation. And the significant results help to further validate the climate construct.

The results supporting both H2a and H2b provide important incremental steps on the path to understanding security climate. First, these results demonstrate that shared perceptions regarding security do develop among employees within a division. This confirms that security climate does emerge as a group level variable. In addition, evidence suggests that security climate varies across divisions and these differences are related in a meaningful way to other measurable security characteristics of the division

(in this case, division security exposure). In light of these findings, it seems reasonable to conclude that security climate exists as a definable construct.

Outcomes of Security Climate

A central assumption underlying much of the research on organizational climate seems to be the notion that the construct influences organizational performance. Schneider (1975) postulated that the general mechanism driving the climate-performance relationship is the human desire for an ordered environment to guide an individual's understanding of the behaviors deemed appropriate by the group to which they belong. In other words, individuals in a group attempt to adjust their behavior to be consistent with the common understanding (i.e. shared perceptions) of what is expected from them. If this common understanding is positive (i.e. in line with the goals of the organization) the resulting behaviors should lead to performance improvement within the group. Likewise, if the common understanding is negative (i.e. counter to the goals of the organization) the resulting behaviors might be detrimental to the group's performance.

On the basis of this logic, the final goal of the study was to investigate the relationship between division security climate and division security performance. To that end Hypothesis 3a proposed that a division's security climate would be negatively related to the frequency of security events within the division, and Hypothesis 3b proposed that a division's security climate would be negatively related to the severity of security events within a division. However, neither hypothesis could be accurately evaluated due to the presence of reciprocal suppression (which occurs when each of the predictor variables in a regression equation simultaneously exert a suppression effect on the other predictor variables in the equation). Unlike other suppression situations where *the* predictor

variable(s) exerting a suppression effect can be identified and removed, in the reciprocal form *all* the predictors act as suppressor variables. As a result, the only reliable estimate of the effect size between a particular predictor and the criterion requires eliminating all other predictors from the analysis to remove the effect of suppression. In the current study, this meant relying on the zero order correlations between security climate and the two security performance metrics.

Tests of H3a produced four validity coefficients between security climate and event frequency. Of the four, only the correlation between Year One climate and Year Two frequency was significant ($r = .26$, $p < .05$, N = 39). Results from H3b produced four validity coefficients between security climate and event severity. The only significant result was the correlation between Year Two climate and Year Two severity ($r = .38$, $p < .05$, N = 38). To extend this discussion, briefly consider the significant validity coefficients from the sixteen supplemental regression analyses that were conducted. When frequency of self-reported events served as the criterion, the correlation between climate in Year Two and self-reporting in Year Three ($r = -.28$, $p < .05$, N = 42) was the only significant finding. The four analyses that used frequency of non-self-reported behavior as the criterion found significant correlations for both of the one year lagged analyses ($r = .31$, $p < .05$, N = 37 and $r = .32$, $p < .05$, N = 41 for the Y1/Y2 and Y2/Y3 lags respectively) but neither of the within year analyses were significant. When reportable events served as the criterion, the correlation between Year Two security climate and Year Three reportable events was significant ($r = -.37$, $p < .05$, N = 41). Finally, when the criterion was sub-reportable events, the only significant result was the

correlation between Year One climate and Year Two sub-reportable events ($r = .30$, $p < .05$, N = 39).

Overall, the analyses conducted to test H3a and H3b combined with the results from the supplemental analyses produced twenty-four zero order correlations between security climate and the criterion measures. A total of seven of these correlations (about 30%) were significant. Clearly, these results do not provide overwhelming support for the existence of a security climate – security performance relationship. But despite these somewhat disappointing findings, the analyses did reveal some interesting patterns in the results that could be useful in the effort to better understanding security climate.

One such pattern points to a counterintuitive relationship between security climate and security performance. Originally a positive relationship between the constructs was proposed where increases in security climate (climate gets stronger) would be accompanied by increases in security performance (frequency of events goes down or average event severity decreases). But the significant correlations between security climate and the two original metrics of security performance seem to suggest that the relationship is in the opposite direction, as security climate increases so does both event frequency and event severity (increases in these criterion measures were viewed as an indication of decreasing security performance).

In truth, a number of explanations could be put forth to account for these counterintuitive results. One possible explanation comes from work done in the field of safety climate by Mearns and colleagues (Mearns, Flin, Gordon, & Fleming, 1998). These authors postulated that in some situations a strong safety climate might create a sense of complacency among employees which might lead to increased safety problems.

While this notion runs counter to the hypotheses put forth in the current study, and perhaps the core assumptions regarding the climate – performance relationship laid out by Schneider (1975), it does provide a potential explanation for the peculiar findings.

However, there are other possible explanations for these results that do not conflict with the initial expectations regarding the direction of a security climate – security performance relationship. For example, it is possible that an increase in security climate could be associated with an increase in employee vigilance, rather than complacency, regarding security. Given the fact that senior security managers within the organization have acknowledged that security events are likely underreported, increased vigilance among employees could result in better detection of security events and/or better compliance with the rules requiring employees to report potential events when they are discovered. This could lead to an increase in the number, and potentially the average severity, of events that get reported even if there is no change in the actual number of events that occur. As a result, it might initially appear as if stronger security climate was related to weaker security performance. However, this initial view would be misleading because the increased employee vigilance – resulting from an increase in security climate – actually leads to a more accurate (although somewhat higher) assessment of the true level of security event frequency and severity. In the end, this explanation of the counterintuitive results is both plausible and not in direct conflict with the initial expectations regarding the direction of a security climate – security performance relationship.

Unfortunately, it is possible to poke holes in both of these potential post-hoc explanations when they are viewed within the context of the significant correlations

attained from the supplemental analyses. Consider, for example, what occurred when the original criterion of event frequency was divided into two separate criterion measures (frequency of self-reported events and frequency of non-self-reported events). While only three significant zero order correlations were found, they showed that stronger security climate was associated with a decrease in the frequency of self-reported events but an increase in non-self-reported events. If a strong climate were to lead to employee complacency, as posited by Mearns et al. (1998), one would expect a positive correlation between security climate and frequency of non-self-reported events rather than the negative correlation that was found. Likewise, when the other original criterion (average event severity) was divided into two separate measures the significant correlations showed that stronger security climate was associated with a decrease in the frequency of reportable events (those ranked as IMI1-IMI4 according to Table 2) but an increase in the frequency of sub-reportable events. If strong security climate leads to better employee vigilance (as discussed above) one would expect a positive correlation between security climate and frequency of reportable events rather than the negative correlation that resulted. In conclusion, any attempt to offer post-hoc explanations for results is rightly viewed as speculation. The surprising results might just as likely be explained by a more complex relationship between variables, the use of a non-normal sample that doesn't reflect the overall population, or some other factor.

Theoretical Implications

There are important theoretical implications to consider as a result of the current project. First, the study proposes and develops the construct of security climate which is a novel application of the general organizational climate concept. In doing so, this work

also addresses the somewhat underserved question of situational factors that might lead to security related events. Finally, the study argues for the existence of a category of workplace behaviors (i.e., security behaviors) that is distinct from similar types of workplace behaviors that are already well established in the organizational science research. Each of these implications will be discussed in greater detail below.

The primary goal of this project was to explore the concept of security climate. Admittedly, some research has explored the general climate construct in relation to specific security events such as theft (Levine & Jackson, 2002). However, this study is one of the first known to propose and investigate a novel application of climate which is focused on the broader strategic organizational outcome of security. Therefore, this effort is theoretically important because it expands the extant field of organizational climate research.

In addition to the theoretical implications associated with developing the construct, the study also has implications for research on topics such as theft. Specifically, it addresses a call made almost two decades ago (Trevino & Youngblood, 1990) for more investigation of the role situational variables play in the occurrence of such events. Before that time, a great deal of attention had been paid to individual level variables such as age (Hollinger, 1986), gender (Mangione & Quinn, 1975), personality (Salgado, 2002), or tenure (Duffy, Ganster, & Shaw, 1998) despite the fact that it is widely accepted that behaviors result from the interaction of both situational and individual factors. While subsequent research has explored situational variables like organizational justice in relation to behaviors such as theft (e.g., Greenberg, 1990), the current study bolsters these efforts by providing some evidence that the situational

variable of security climate may be another important factor which contributes to the occurrence of security related events.

In addition, the current study directly addresses the relationship between security behaviors and the concepts of CWBs and safety behaviors. Admittedly there are similarities, and in some cases an overlap, between security behaviors and the other two concepts. However, the case was made that security behaviors should be viewed as a distinct category of workplace behaviors. This argument is theoretically important because it suggests that the existing nomological network (Cronbach & Meehl, 1955) covering workplace behaviors should be expanded to include a unique category covering security behaviors which would be operationalized through the three separate dimensions of perpetrator (organizational insider, outsider, or some combination of the two), target (a continuum from organizational assets to individual assets), and intention (behaviors can range from non-nefarious error to malicious intent).

Practical Implications

In addition to the theoretical implications above, the study suggests a number of practical implications as well. For example, the system for categorizing security events (perpetrator, target, and intention) proposed earlier might be a useful tool for professionals in the security field. Admittedly, many security conscious organizations conduct investigations which gather a wealth of information that could be used to categorize events. But despite the important role of human behavior in security events (Pond, 2002), common classification systems used by security practitioners (e.g., the IMI system for rating event severity used by the organization in this study) do not address the factors that drive those behaviors. Therefore, incorporating the proposed classification

system into existing security investigations may help security professionals begin to identify not only how certain types of security events occur, but also why they occur.

A second practical implication from the study deals with recommendations from groups such as the IAEA (e.g., IAEA, 2001; IAEA, 2002; IAEA, 2003) which advocate more focus on organizational factors when establishing security in the nuclear environment. These IAEA recommendations might be justified, but up until now the organization has not provided concrete explanations of constructs such as security climate. Furthermore, the validity of these suggestions has not been investigated empirically. Therefore, the results of this study are important because they suggest caution for security professionals who hope to utilize security climate in order to improve security performance. Based on the study results, it could be argued that the findings do not yet justify dedicating resources to security climate in an applied setting. This is not to say that there is no meaningful security climate – security performance relationship, it simply means that at this early stage the true relationship between the two is not clear. Therefore, in the nuclear environment (which is high-risk and high-consequence), broad statements about the utility of security climate should be tempered until more robust conclusions can be made.

Limitations

As with all research, this study contains some limitations that must be acknowledged. First of all, the analyses which used data aggregated at the division level (i.e. H2b, H3a and H3b) suffer from a relatively small sample sizes. Furthermore, the sample size was restricted to the number of division within the organization (minus

divisions with missing data). With that in mind, interpretation of the results should be done cautiously because estimates of effect size can be unstable when *N* is low.

In addition to sample size, some of the measures used in the study also create potential limitations. In the Results section above, I discussed the near-perfect correlation between the ratings of security exposure in Year Two and Year Three and the possibility that this result was due to the way exposure data was collected (SMEs ratings for both years collected at the same time, more than two years after Year Three). However, the type of work done in a division does not change much from one year to the next so there is reason to believe that exposure wouldn't change much either. Likewise, the interrater reliability results were acceptable for both years. Ideally, more objective measures of security exposure (e.g., percentage of a division's employees with government security clearances) would have been preferred but were not made available by the study organization. Despite this, the evidence does provide some confidence in the exposure measure.

The measure of security climate also had some limitations. As mentioned previously, the measure contained only three items and only two of the three dimensions proposed in H1a-H1b were represented. Clearly, additional items would have been desirable as this would have allowed for more thorough sampling of the content domain and possibly improved the reliability of the measure. Nonetheless, the security climate scale did exhibit sound psychometric properties.

In addition, there are potential limitations associated with the criterion measures of security performance. All of these measures (the two originally proposed and the four created for the supplemental analyses) were derived from the Event data set supplied by

the organization's Security Division. This data set contained information about all of the security events that the organization knew about, but it is likely that the data set did not include every event that occurred. There are two factors that may account for this fact. First, those security events that occur as a result of malevolent intent, while rare, are almost always surreptitious in nature. That is, those individuals who violate security procedures for nefarious purposes (e.g., an espionage agent of a foreign government or an employee stealing assets for personal gain) will only succeed in their efforts if they are able to avoid detection. Furthermore, those events that are neither intentional nor malevolent may not always be detected. While employees in the organization have a responsibility to report any potential events, doing so can result in punitive action against those involved.

One common alternative to formal event reports, upon which the Event data set in the current study is based, is the use of surveys where respondents answer questions about their own involvement in activities such as workplace theft or other CWBs (e.g., Hollinger, 1986; Slora, 1989). In theory, this method of data collection will likely provide the lowest-bound estimates of event base rates because the truthfulness of answers on sensitive topics have been questioned (e.g., Dalton & Metzger, 1992). For example, an elegantly designed study conducted by Wimbush and Dalton (1997) used three separate methods to estimate base rates of workplace theft. The three methods utilized by the authors included anonymous surveys, the randomized-response technique (RRT), and an unmatched-count technique (UCT). The results demonstrated that the estimates of overall theft rates obtained from the RRT and UCT methods were virtually identical (59.2% and 57.9% respectively). However, participants' admissions of theft

behavior from the survey produced an estimated base rate of 28.2% which was less than half that of the other two methods. The authors suggest that these results might be attributed to participants' perceptions of anonymity in each of the three methods. Survey respondents may question the assertion of anonymity in the survey method. However, data collected using the RRT and UCT methods only have meaning when viewed in aggregate so even if individuals' responses were not anonymous it would be impossible to determine whether any single individual participated in workplace theft.

Because there is no expectation of anonymity in the formal process of event reporting within the study organization, it is logical to assume the Event data set might underestimate the true number of security events. Under the current circumstance, it is impossible to know how many security events go undiscovered by the organization over the course of a year so it is difficult to determine the accuracy of the Event data set. However, characteristics of the organization and its workforce exist which are believed to minimize this issue. First, the organization's work environment is high regulated and employees' activities are closely monitored for possible security violations. Likewise, audits are frequently conducted by the Security Division which can lead to the discovery of unreported security violations. In addition, employees generally take their responsibility for self-reporting potential security violations very seriously because when an event is not self-reported but is discovered anyway, any punitive action that would have been taken against an employee for their involvement can be dramatically increased. Furthermore, all employees are required to report possible security violations committed by co-workers – which mirrors the use of both self- and peer-reporting of CWBs in previous research (e.g., Penney & Spector, 2005) – and individuals can be held

accountable for failing to do so. Ultimately, the data set was the most complete record of security events available which is why it was used to derive metrics of security performance.

One final limitation to the study was the fact that demographic information from the employee opinion survey was not available for inclusion as study variables due to privacy concerns raised by the organization. Because previous research has found that individual difference variables such as age (Hollinger, 1986) and gender (Mangione & Quinn, 1975) are correlated to behaviors such as theft and sabotage, the inclusion of such demographic variables might have added to the current study.

Future Research

The limited amount of empirical research aimed at investigating security climate means that a number of unanswered questions about the construct remain. In light of this, the field seems to have great potential for future research. One area that seems to merit further exploration is the dimensional structure of the construct. The nature of the data used in this study restricted the types of dimensions that could be explored. But considering the wide variety of climate dimensions that have been proposed (e.g., Ostroff et al., 2003), additional dimensions of security climate beyond those included here are certainly possible. Therefore, future research should not only attempt to replicate the current study results, it should also investigate whether other facets not mentioned in this study might be important components of climate for security.

There are a variety of potential security climate dimension worthy of consideration including perceptions of the organization's security professionals, workplace and job demands, and even employees' perceptions risk. In fact, risk

perceptions have already been explored as a dimension of safety climate. For example, DeJoy (1996) conceptualized employees' perceptions of risk – what he termed "hazard appraisal" – as an important component of climate for safety which lead employees to adopt self-protective behaviors such as the use of personal protection equipment. In addition, Weyman et al. (2003) factor analyzed responses from coal miners on an eighty-three item safety survey. Results indicated a three-factor structure where "confidence in ability to control risk" was one factor.

But while evidence from the safety field bolsters the claim that the dimension may also prove to be an important component of security climate, perceptions of security risk may be more complex than perceptions of safety risk. In terms of safety, the risk is usually viewed as a risk to oneself and perhaps to other co-workers ("Will I, or my co-workers, get hurt doing this job?"). In contrast, risk in the security context can be viewed in multiple ways. On the one hand, employees' perceptions may focus on risks to themselves or co-workers when their actions cause security events ("Will I get caught and be punished for negative security behaviors?"). On the other hand, employees' perceptions could also focus on the risks faced by the organization ("Is the organization really under credible threat?"). In the end, investigation of each of these types of employee perceptions will lead to a better understanding of the security climate construct.

A related issue that needs additional research attention is the development and validation of a measure designed specifically to assess climate for security. The development of measures specific to climate for security would make it easier for future researchers attempting to further explore the nature of the concept. To construct such a measure, future research might focus on developing items to assess the three security

climate dimensions proposed in the current study. More specifically, each dimension's content domain could serve as a starting point in the process of item development.

For example, a review of the SME responses that were sorted into the management commitment to security category revealed that multiple SMEs had talked about the importance of managers modeling good security behavior, providing adequate resources to meet security objectives, and communicating regularly with employees regarding security matters. Common themes from the co-worker support for security category included the importance of both co-worker attitudes about security (particularly the attitudes of well respected co-workers) as well as the willingness of co-workers to intervene when they witness poor security behaviors from peers. Finally, within the security policies and procedures category common themes included the importance of involving employees in the development of these policies and procedure, avoiding the proliferation of confusing and sometimes inconsistent policies and procedures, and assuring fairness in the way the organization responds after an incident has occurred.

Future efforts to study climate for security might also consider the question of generalizability. The organization at the center of this study is unique for a variety of reasons. For example many of the organization's employees hold high-level government security clearances, the work that they conduct is often sensitive, and the organization has a strong security program in place. While these characteristics combine to create a fascinating environment for security research, they also present uncertainty about the generalizability of study results. For example, financial institutions, retail organizations, and hospitals all face important security issues but the nature of these issues (such as the kinds of adversaries they are confronted with and the threats posed by these adversaries)

are likely to vary significantly from those of the organization in this study. As a result, future research might investigate organizational differences in areas such as the way security climate develops, the relative importance of different dimensions, and how security climate might influence security behaviors.

Another area for future research is the need for cross-cultural investigations of security climate. As mentioned previously, the IAEA has repeatedly stressed the importance of organizational factors at nuclear facilities (e.g., IAEA, 2001; IAEA, 2002; IAEA, 2003) around the globe. Such calls lead to important cross-cultural questions that should be addressed. For example, in the field of nuclear security it has been suggested that constructs such as security climate would be most useful if some type of "world norms" could be established (R. Lawrence, personal communication, January 28, 2008). However, developing international standards for security climate might prove to be difficult. On the one hand, different cultures tend to view the concept of security differently (Khripunov, 2005). In addition, ideas about security could potentially be impacted by cultural dynamics such as Hofstede's (1983) proposition that nations can vary on a continuum from individualism (each person is responsible for themselves and commitment to the group is secondary) to collectivism (loyalty to the group is expected in exchange for the benefits that membership affords). Therefore, it may be possible that while many aspects of security climate are equally relevant in any country, some aspects of the construct may need to be tailored to the unique perspectives of a given culture. As a result, cross-cultural differences in the type of security climate that emerges (or in the process of emergence itself) ought to be explored.

The final area for potential future research is to examine how the presence of a security climate might affect other types of climates as well as how it might interact with other climates and impact organizational outcomes. According to Ostroff et al. (2003), most of the research that examines specific climate types (e.g., safety climate) does so while ignoring other types of climate that may also be present at the same time. Therefore, it is worth examining how the presence of a security climate might interact with other types of climates and these interactions might impact organizational outcomes.

As suggested recently by Zohar (2008), organizational climate contains multiple facets such as ethical climate (Parboteeah & Kapp, 2008), customer service climate (Schneider, 1990), and violence climate (Spector, Coulter, Stockwell, & Matz, 2007). It is possible that some of these climates would likely covary because they reflect different yet related organizational characteristics. Based on Zohar's multi-climate framework, security climate may interact with ownership climate, which indicate whether organizations encourage workers to commit extra-role activities such as vigilance or focus on workers' compliance on every security regulations (i.e., in-role activity). Under the high security climate and high ownership climate, workers would show extra-role or citizenship security behaviors. In contrast, workers would comply with security regulations as required when security climate is high and ownership climate is low.

Another example would be the relationship between security climate and climate for innovation. On the one hand, a strong security climate might lead employees to be cautious about widely disseminating sensitive information. However, innovative climates tend to exhibit a free flow of information. Given that these two perspectives

appear to be at odds, it is likely that these climates would affect each other such that a strong security climate would hinder a strong innovative climate, or vice versa.

It is not overstated to say that the study of security climate is very much in its infancy. Therefore, there is great potential for future research in the field. While I have tried to lay out my vision of important areas needing additional study, there is no doubt that there are many other avenues that have not been mentioned.

Conclusion

The establishment of good security has been a focus of societies throughout history (Johnston, 2006). To support these efforts within the context of the organization, the current study sought to empirically investigate the novel construct of climate for security. In doing so, a number of important milestones in the development of the construct were reached. First, by adapting the generally accepted definition of organizational climate to the specific strategic outcome of security it was possible to define security climate as a security characteristic of an organization that is manifested in employees' shared perceptions of the organization's security policies, practices, and procedures. In addition, the construct was further operationalized by identifying three dimensions including management support for security, co-worker support for security, and perceptions of security policies and procedures. Furthermore, a basic measure of security climate was identified and the emergence of security climate was confirmed. Finally, a preliminary exploration of potential relationships between security climate and security performance was conducted. In light of these accomplishments, it is reasonable to conclude that the three primary goals of the study (developing the construct, evaluating

its emergent nature, and exploring the relationship between security climate and security performance) were achieved.

Admittedly, however, the study did have limitations which put constraints on what could be accomplished. And in some cases, perhaps due to the exploratory nature of the study, the results raised almost as many (if not more) questions than they were able to answer. Therefore, it is clear that much more research is needed to further develop and refine the construct. Nevertheless, the findings of the study suggest that security climate could be a useful component of an organization's overall security strategy.

References

Amabile, T. M., Conti, R., Coon, H., Lazenby, J., & Herron, M. (1996). Assessing the work environment for creativity. *Academy of Management Journal, 39*(5), 1154-1184.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Eds.), *Action-control: From cognition to behavior* (pp. 11- 39). Heidelberg, Germany: Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179-211.

Ashforth, B. (1985). Climate formation: Issues and extensions. *Academy of Management Review, 18*(4), 837-847.

Bartko, J. J. (1976). On various intraclass correlation reliability coefficients. *Psychological Bulletin, 83*, 762-765.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin, 107*, 238-246.

Bentler, P. M. (1992). On the fit of models to covariances and methodology to the *Bulletin*. *Psychological Bulletin, 112*(3), 400-404.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin, 88*, 588-606.

Bird, F. E., & Germain, G. L. (1996). *Practical Loss Control Leadership.* Loganville, GA: Det Norske Verita.

Blau, P. M. (1964). *Exchange and power in social life*. New York: Wiley.

Campbell, J. P., Dunnette, M. D., Lawler, E. E., & Weick, K. E. (1970). *Managerial behavior, performance, and effectiveness.* New York: McGraw-Hill.

Campbell, D., & Fiske, D. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin, 56*(2), 81-105.

Carr, J. Z., Schmidt, A. M., Ford, J. K., & DeShon, R. P. (2003). Climate perceptions matter: A meta-analytic path analysis relating molar climate, cognitive and

affective states, and individual level work outcomes. *Journal of Applied Psychology, 88*(4), 605-619.

Carter, N., Holmström, A., Simpanen, M., & Melin, L. (1988). Theft reduction in a grocery store through product identification and graphing of losses for employees. *Journal of Applied Behavior Analysis, 21*(4), 385-389.

Case, J. (2000). *Employee theft: The profit killer.* Del Mar, CA: John Case & Associates.

Cherrington, D. J., & Cherrington, J. O. (1985). The climate of honesty in retail stores. In W. Terris (Ed.), *Employee theft: research, theory and applications* (pp.27-39). Park Ridge, IL: London House.

Clarke, S. (1999). Perceptions of organizational safety: Implications for the development of a safety culture. *Journal of Organizational Behavior, 20*(2), 185-198.

Coffin, B. (2003). Breaking the silence on white collar crime [Electronic version]. *Risk Management, 50*(9), 8.

Cohen, J. A. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement, 20*, 37-46.

Cohen, J. A. (1968). Weighted kappa: Nominal scale agreement with provision for scaled disagreement or partial credit. *Psychological Bulletin, 70*(4), 213-220.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences (3rd ed.)*. Mahwah, NJ: Lawrence Erlbaum Associates.

Conger, A. J. (1974). A revised definition for suppressor variables: A guide to their identification and interpretation. *Education and Psychological Measurement, 34*, 35-46.

Coyle, I. R., Sleeman, S. D., & Adams, N. (1995). Safety climate. *Journal of Safety Research, 26*(4), 247-254.

Cree, T., & Kelloway, E. K. (1997). Responses to occupational hazards: Exit and participation. *Journal of Occupational Health Psychology, 2*(4), 304-311.

Crocker, L., & Algina, J. (1986). *Introduction to classical and modern test theory*. Belmont, CA: Wadsworth.

Cronbach, L., & Meehl, P. (1955). Construct validity in psychological tests, *Psychological Bulletin, 52*(4), 281-302.

Dabney, D. (1995). Neutralization and deviance in the workplace: Theft of supplies and medicines by hospital nurses. *Deviant Behavior, 16*(4), 313-321.

Dalton, D. R., & Metzger, M. B. (1992). Towards candor, cooperation, and privacy in applied business ethics. *Business Ethics Quarterly, 2*, 207-221.

Darlington, R. B. (1968). Multiple regression in psychological research and practice. *Psychological Bulletin, 69*, 161-182.

DeJoy, D. M. (1996). Theoretical models of health behavior and workplace self-protective behavior. *Journal of Safety Research, 27*(2), 61-72.

Diaz, R. I., & Cabrera, D. D. (1997). Safety climate and attitude as evaluation measures of organizational safety. *Accident Analysis and Prevention, 29*(5), 643-650.

Duffy, M. K., Ganster, D. C., & Shaw, J. D. (1998). Positive affectivity and negative outcomes: The role of tenure and job satisfaction. *Journal of Applied Psychology, 83*(6), 950-959.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Fleiss, J. L. (1971). Measuring nominal scale agreement among many raters. *Psychological Bulletin, 76*(5), 378-382.

Flin, R., Mearns, K., O'Connor, P., & Bryden, R. (2000). Measuring safety climate: Identifying the common features. *Safety Science, 34*, 177-192.

Greenberg, J. (1997) A social influence model of employee theft: Beyond the fraud triangle. *Research on Negotiations in Organizations, 6*, 29-51.

Greenberg, J. (1990). Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts. *Journal of Applied Psychology, 75*(5), 561-568.

Greenberg, J. & Scott, K. S. (1996). Why do workers bite the hands that feed them? Employee theft as social exchange process. *Research in Organizational Behavior, 18*, 111-156.

Griffin, M. A. & Neal, A. (2000). Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge, and motivation. *Journal of Occupational Health Psychology, 5*(3), 347-358.

Gruys, M. L. (1999). *The dimensionality of deviant employee performance in the workplace*. Unpublished doctoral dissertation, University of Minnesota.

Guastello, S. J., & Guastello, D. D. (1988). *The Occupational Hazards Survey: Second Edition Manual and Case Report*. Milwaukee, WI: Guastello & Guastello.

Heinrich, H. W. (1931). *Industrial accident prevention: A scientific approach.* New York: McGraw-Hill.

Hemingway, M. A., & Smith, C. S. (1999). Organizational climate and occupational stressors as predictors of withdrawal behaviors and injuries in nurses. *Journal of Occupational and Organizational Psychology, 72*, 285-299.

Ho, M. (2005). *Safety climate and occupational injury: An examination of climate dimensions and injury outcomes.* Unpublished doctoral dissertation, The Johns Hopkins University, United States -- Maryland. Retrieved June 5, 2007, from ProQuest Digital Dissertations database. (Publication No. AAT 3155623).

Hobijn, B., & Sager, E. (2007). What has homeland security cost? An assessment: 2001-2005 [Electronic version]. *Current Issues in Economics and Finance, 13*(2), 1-7. New York: Federal Reserve Bank of New York.

Hofmann, D. A., & Morgeson, F. P. (1999). Safety-related behavior as a social exchange: The role of perceived organizational support and leader-member exchange. *Journal of Applied Psychology, 84*(2), 286-296.

Hofmann, D. A., Morgeson, F. P., & Gerras, S. J. (2003). Climate as a moderator of the relationship between leader-member exchange and content specific citizenship: Safety climate as an exemplar. *Journal of Applied Psychology, 88*(1), 170-178.

Hofstede, G. (1983). "Dimensions of national cultures in fifty countries and three regions." In J. B. Deregowski, S. Dziurawiec, and R. C. Annis (eds.), *Expiscations in Cross-Cultural Psychology*: 335 355. Lisse, Neth.: Swets and Zeitlinger.

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

Hollinger, R. C. (1989). *Dishonesty in the Workplace: A manager's guide to preventing theft.* Park Ridge, IL: London House.

Hollinger, R. C., & Clark, J. P. (1982). Formal and informal social controls of employee deviance. *The Sociological Quarterly, 23*(3), 333-343.

Homans, G. C. (1958). Social Behavior as Exchange. *American Journal of Sociology, 63*, 597-606

Horning, D. (1970). Blue collar theft: Conceptions of property deviance, attitudes toward pilfering, and work group norms in a modern industrial plant. In E. O. Smigel &

H. L. Ross (Eds.), *Crimes Against Bureaucracy* (pp. 46-64). New York: Van Nostrand Reinhold.

Horst, P. (1941). The role of the predictor variables which are independent of the criterion. *Social Science Research Council, 48*, 431-436.

Huang, Y., Chen, J., DeArmond, S., Cigularov, K., & Chen P. (2007). Roles of safety climate and shift work on perceived injury risk: A multi-level analysis. *Accident Analysis and Prevention, 39*, 1088-1096.

International Atomic Energy Agency: Board of Governors. (2001, August). *Nuclear verification and security of material: Physical protection objectives and fundamental principles* (GOV/2001/41). Vienna, Austria.

International Atomic Energy Agency: Board of Governors/General Conference. (2002, September). *Measures to strengthen international cooperation in nuclear, radiation, transport and waste safety: Implementation of the revised action plan for the safety and security of radiation sources* (GOV/2002/35/Add. 1 - GC46/11/Add. 1). Vienna, Austria.

International Atomic Energy Agency: General Conference. (2003, August). *Nuclear security: Measures to protect against nuclear terrorism* (GC47/17). Vienna, Austria.

Jackofsky, E. F., & Slocum, J. W. (1988). A longitudinal study of climates, *Journal of Organizational Behavior, 9*(4), 319-334.

James, L. R., Demaree, R. J., & Wolf, G. (1984). Estimating within-group interrater reliability with and without response bias. *Journal of Applied Psychology, 69*(1), 85-98.

James, L. R., Demaree, R. J., & Wolf, G. (1993). r_{wg}: An assessment of within-group interrater agreement. *Journal of Applied Psychology, 78*(2), 306-309.

James, L. R., & Jones, A. P. (1974). Organizational climate: A review of theory and research. *Psychological Bulletin, 81*, 1096-1112.

Johnston, R. G. (2006). Tamper-indicating seals. *American Scientist, 94*(6), 515-523.

Jones, J. W., & Terris, W. (1983). Predicting employees' theft in home improvement centers. *Psychological Reports, 52*(1), 187-201.

Khripunov, I. (2005). Nuclear security: Attitude check. *Bulletin of the Atomic Scientists, 61*(1), 58-64.

Khripunov, I., Nikonov, D., & Katsva, M. (2004). *Nuclear security culture: The case of Russia*. Khripunov, I., & Holmes, J. (Eds.). Athens, GA: University of Georgia, Center for International Trade and Security.

King, J. E. (2004). Calculating a generalized kappa statistic for use with multiple raters [Microsoft Excel file]. Retrieved on February 29, 2008 from http://www.ccitonline.org/jking/homepage/kappa.xls

Kipfer, B. A. (Ed.). (2007). *Roget's New Millennium Thesaurus* (1st Edition, v 1.3.1). Retrieved April 9, 2007, from Thesaurus.com website: http://thesaurus.reference.com/browse/security.

Kozlowski, S. W. J., & Klein, K. J. (1987). An exploration of climates for technical updating and performance. *Personnel Psychology, 40*, 539-563.

Kozlowski, S. W. J., & Klein, K. J. (2000). A multilevel approach to theory and research in organizations: Contextual, temporal, and emergent processes. In K. Klein & S. Kozlowski (Eds.), *Multilevel theory, research, and methods in organizations: Foundations, extensions, and new directions* (pp. 3-90). San Francisco, CA: Jossey-Bass.

Lee, C. (2006, May 26). Worker often took data home; VA tracks practice to 2003; $50,000 reward set for computer. *The Washington Post*, A19.

Levine, S. Z., & Jackson, C. J. (2002). Aggregated personality, climate and demographic factors as predictors of departmental shrinkage. *Journal of Business and Psychology, 17*(2), 287-297.

Lewin, K., Lippitt, R., & White, R. K. (1939). Patterns of aggressive behavior in experimentally created "social climates." *Journal of Social Psychology, 10*, 271-299.

Mangione, T. W., & Quinn, R. P. (1975). Job satisfaction, counterproductive behavior, and drug use at work. *Journal of Applied Psychology, 60*(1), 114-116.

Marquand, R., & Arnoldy, B. (2007, September 14). China emerges as leader in cyberwarfare. *Christian Science Monitor*, p. 1.

McGregor, R., & Sevastopulo, D. (2007, September 4). China 'hacked' into Pentagon defense system. *Financial Times* (London), p. 1.

McGurn, S. (1988, March, 7). Spotting the thieves who work among us. *Wall Street Journal*, p. 16A.

Mearns, K., Flin, R., Gordon, R., & Fleming, M. (1998). Measuring safety climate on offshore installations. *Work & Stress, 12*(3), 238-254.

Meyer, H. H. (1968). Achievement motivation and industrial climates. In R. Taguiri and G. H. Litwin (Eds.), *Organizational climate: Explorations of a concept.* Boston: Division of Research, Graduate School of Business Administration, Harvard University.

Morgenstern, D. (1977). *Blue Collar Theft in Business and Industry.* Springfield, VA: National Technical Information Service.

Neuman, J. H., & Baron, R. A. (1998). Workplace violence and workplace aggression: Evidence concerning specific forms, potential causes, and preferred targets. *Journal of Management, 24*, 391-319.

Occupational Safety and Health Act (1970). http://www.osha.gov/pls/oshaweb/owasrch.search_form?p_doc_type=OSHACT

Ostroff, C., Kinicki, A. J., & Tamkins, M. M. (2003). Organizational culture and climate. In I. B. Weiner (Series Ed.) & W. C. Borman, D. R. Ilgen, & R. J. Klimoski (Vol. Eds.), *Handbook of psychology: Vol. 12. Industrial and organizational psychology* (pp. 565-593). Hoboken, NJ: John Wiley & Sons.

Parboteeah, K., & Kapp, E. (2008). Ethical climates and workplace safety behaviors: An empirical investigation. *Journal of Business Ethics*, *80*(3), 515-529.

Payne, R. L., & Pugh, D. S. (1976). Organizational structure and climate. In M. D. Dunnette (Ed.), *Handbook of Industrial and Organizational Psychology* (pp. 1125-1174). Chicago: Rand McNally.

Penney, L. M., & Spector, P. E. (2005). Job stress, incivility, and counterproductive work behavior (CWB): The moderating role of negative affectivity. *Journal of Organizational Behavior, 26*, 777-796.

Pond, D. J. (2002). *Enhanced Security Through Human Error Reduction (ESTHER)*, LA-UR-02-815. Los Alamos, NM: Los Alamos National Laboratory.

Pritchard, R. D., & Karasick, B. W. (1973). The effects of organizational climate on managerial job performance and job satisfaction. *Organizational Behavior and Human Performance, 9*, 126-146.

Reichers, A. E., & Schneider, B. (1990). Climate and culture: An evolution of constructs. In B. Schneider (Ed.), *Organizational climate and culture* (pp. 5-39). San Francisco: Jossey-Bass.

Rentsch, J. R. (1990). Climate and culture: Interaction and qualitative differences in organizational meanings. *Journal of Applied Psychology, 75*, 668-681.

Rigdon, J. E. (1994). Companies see more workplace violence. *Wall Street Journal,* April 12: B1.

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal, 38*(2), 555-572.

Sackett, P. R. (2002). The structure of counterproductive work behaviors: Dimensionality and relationships with facets of job performance. *International Journal of Selection and Assessment, 10*(1/2), 5-11.

Sackett, P. R., & DeVore, C. J. (2002). Counterproductive behaviors at work. In N. Anderson, D. S. Ones, H. K. Sinangil, & C. Viswesvaran (Eds.), *Handbook of Industrial, Work, and Organizational PsychologyVolume 1: Personnel Psychology* (pp. 145-164). Thousand Oaks, CA: Sage Publications Ltd.

Salgado, J. F. (2002). The big five personality dimensions and counterproductive behaviors. *International Journal of Selection and Assessment, 10*(1/2), 117-125.

Schneider, B & Bartlett, C. J. (1968). Individual differences and organizational climate: I. The research plan and questionnaire development. *Personnel Psychology, 21*, 323-333.

Schneider, B. (1975). Organizational climates: An essay. *Personnel Psychology, 28*, 447-479.

Schneider, B. (1990). The climate for service: An application of the climate construct. In B. Schneider (Ed.), *Organizational Climate and Culture* (pp. 383-412). San Francisco: Jossey Bass.

Schneider, B., & Hall, D. T. (1972). Toward specifying the concept of work climate: A case study of Roman Catholic diocesan priests. *Journal of Applied Psychology, 56*, 447-455.

Schneider, B., & Reichers, A. E. (1983). On the etiology of climates. *Personnel Psychology, 36*(1), 19-39.

Schneider, B., & Snyder, M. (1975). Some relationships between job satisfaction and organizational climate. *Journal of Applied Psychology, 60*, 318-328.

Schneider, B., White, S. S., & Paul, M. C. (1998). Linking service climate and customer perceptions of service quality: Test of a causal model. *Journal of Applied Psychology, 83*, 150-163.

Seo, D. C., Torabi, M. R., Blair, E. H., & Ellis, N. T. (2004). A cross-validation of safety climate scale using confirmatory factor analytic approach. *Journal of Safety Research, 35*, 427-445.

Seper, J. (2007, February 13). Ten of 160 missing FBI laptops had sensitive data. *The Washington Times*, p. A3.

Shrout, P. E., & Fleiss, J. L. (1979). Intraclass correlations: Uses in assessing rater reliability. *Psychological Bulletin, 86*, 420-428.

Sieh, E. W. (1987). Garment workers: Perceptions of inequity and employee theft. *The British Journal of Criminology*, *27*(2), 174-190.

Silva, S., Lima, M. L., & Baptista, C. (2004). OSCI: An organisational and safety climate inventory. *Safety Science, 42*, 205-220.

Simpson, J., & Weiner, E. (Eds.). (1989). Oxford English Dictionary (2nd. Ed., OED Online). Oxford, UK: Oxford University Press. Retrieved October 15, 2007 from http://0-dictionary.oed.com.catalog.library.colostate.edu/cgi/entry/50218187?single=1&query_type=word&queryword=security&first=1&max_to_show=10.

Slora, K. B. (1989). An empirical approach to determining employee deviance base rates. *Journal of Business and Psychology, 4*(2), 199-219.

Smith-Crowe, K., Burke, M. J., & Landis, R. S. (2003). Organizational climate as a moderator of safety knowledge-safety performance relationships. *Journal of Organizational Behavior, 24*, 861-876.

Snyder, L. A., Chen, P. Y., Grubb, P. L., Roberts, R. K., Sauter, S. L., & Swanson, N. G. (2004). Workplace aggression and violence: causes, consequences, and interventions. In P. L. Perrewe and D. C. Ganster (Eds.). *Research in Occupational Stress and Well Being, 4*, 1-65.

Spector, P. E. (1975). Relationships of organizational frustration with reported behavioral reactions of employees. *Journal of Applied Psychology, 60*, 635-637.

Spector, P. E., Coulter, M. L., Stockwell, H. G., & Matz, M. W. (2007). Perceived violence climate: A new construct and its relationship to workplace physical violence and verbal aggression, and their potential consequences. *Work & Stress, 21*, 117-130.

Spector, P. E., Fox, S., Penney, L. M., Bruursema, K., Goh, A., & Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviors created equal? *Journal of Vocational Behavior, 68*, 446-460.

Steiger, J. H. (1990). Structural model evaluation and modification: An interval estimation approach. *Multivariate Behavioral Research, 25*, 173-180.

Thornton, G. C. (1969). The dimensions of organizational climate of office situations. Experiential Publication System, 2, 057A.

Tracey, J. B., & Tews, M J. (2005). Construct validity of a general training climate scale. *Organizational Research Methods, 8*, 353-374.

Trevino, L. K., & Youngblood, S. A. (1990). Bad apples in bad barrels: A causal analysis of ethical decision-making behavior. *Journal of Applied Psychology, 75*, 378-385.

Tuckman, B. W. (1965). Developmental sequence in small groups. *Psychological Bulletin, 63*, 384-399.

U.S. Department of Energy (2001). DOE N 471.3. Retrieved June 20, 2006, from http://www.directives.doe.gov/pdfs/doe/doetext/neword/471/n4713.pdf.

Warner, J. S., & Johnston, R. G. (2002). A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *The Journal of Security Administration, 25*, 19-28.

Warner, J. S., & Johnston, R. G. (2006). *Limitations and vulnerabilities of RFID and contact memory devices*. Talk given at the 7th Security Seals Symposium, February 28-March 2; Santa Barbara, CA.

Waters, L. K., Roach, D., & Batlis, N. (1974). Organizational climate dimensions and job-related attitudes. *Personnel Psychology, 27*, 465-476.

Weyman, A., Clarke, D. D., & Cox, T. (2003). Developing a factor model of coal miners' attributions on risk-taking at work. *Work and Stress, 17*(4), 306-320.

White House: Office of the Press Secretary. (2005). Joint statement by President Bush and President Putin on nuclear security cooperation. Retrieved May 26, 2005 from http://www.whitehouse.gov/news/releases/2005/02/20050224-8.html

Wimbush, J. C., & Dalton, D. R. (1997). Base rate for employee theft: Convergence of multiple methods. *Journal of Applied Psychology, 82*(5), 756-763.

Zohar, D. (1980). Safety climate in industrial organizations: Theoretical and applied implications. *Journal of Applied Psychology, 65*(1), 96-102.

Zohar, D. (2000). A group-level model of safety climate: Testing the effect of group climate on microaccidents in manufacturing jobs. *Journal of Applied Psychology, 85*, 587-596.

Zohar, D. (2002). Modifying supervisory practices to improve subunit safety: A leadership-based intervention model. *Journal of Applied Psychology, 87*, 156-163.

Zohar, D. (2008, March). A multi-level multi-climate approach for safety climate. In P. Y. Chen (Chair), *New developments in the conceptualization of safety climate*. Symposium presented at the 7th International Conference on Occupational Stress & Health, Washington, DC, USA.

Appendix A: Instructions for SME Data Set Sorting Task

The table beginning on the next page of this document consists of five columns that you will use to complete the item sorting task. Each of the columns contain descriptive headers. An explanation of each of these columns follows.

Column A/Interview Responses – This column consists of a list of responses collected during semi-structured interviews with a number of subject matter experts (SMEs) in the field of organizational security.

Column B/Management Support –You will use this column to indicate if the responses in Column A are exemplars of Perceptions of Management Support for Security. We define management support as employees' perceptions of the degree to which managers and supervisors support, promote, manage and prioritize the importance of organizational security.

Column C/Co-Worker Support –You will use this column to indicate if the responses in Column A are exemplars of Perceptions of Co-Worker Support for Security. We define co-worker support as employees' perceptions of the degree to which co-workers and peers support, promote, and prioritize the importance of organizational security.

Column D/Policies and Procedures –You will use this column to indicate if the responses in Column A are exemplars of Perceptions of Security Policies and Procedures. We define policies and procedures as employees' perceptions of security policies and procedures including such things as relevance, effectiveness, and user-friendliness.

Column E/Not Applicable –You will use this column to indicate if the responses in Column A are NOT examples of any of the above categories

PROCEDURE: Please carefully read each of the responses in Column A one at a time. After that, decide if the response reflects one of the three categories (as defined above and in the column descriptive headers in Columns B, C, and D) and indicate your choice by marking an X in the corresponding column. If you feel that the response is not an exemplar of any of the three categories, mark an X on Column E. Please mark ONLY ONE X in each row.

The sorting task begins on the next page.