Managerial Tolerance of Insider Information Sabotage Acts and How Different Organizational Cultures Might Influence such Tolerance

Thomas Martin
&
John C. Hafer
University of Nebraska at Omaha

Abstract

The purpose of this mixed-method study is to quantitatively investigate managers' attitudinal tolerance of nineteen acts of information sabotage and then to qualitatively hypothesize what types of organizational culture or cultures might govern those tolerance attitudes in accordance with the concept of Dual Culture Theory or Grid/Group Culture Theory. Managers from numerous organizations across the country were surveyed using a mail survey. Exploratory factor analysis yielded four factors showing varying degrees of managerial tolerance/intolerance. A "hierarchical culture" was hypothesized for the most severe and overt acts, but either an "egalitarian" or "individualistic culture" was hypothesized for the more covert acts that could be mistakenly overlooked as simple mistakes. Discussions and suggestions for future research and applications of Dual Culture Theory conclude this study.

Keywords: *Dual Culture or Grid/Group Culture Theory, Mixed-Method Research, Information Sabotage Acts, Organizational Culture, Managerial Tolerance*

Introduction

Information sabotage, in its various forms, represents different types of data and/or security breaches that have now become wide spread (Bressler & Bressler, 2015) and have occurred in almost every type of industry (e.g., Holtfreter & Harrington, 2015). The Privacy Rights Clearinghouse organization (PRCH) has classified these breaches into one of six categories—1) unintended disclosure, 2) hacking or malware by outside parties, 3) payment card fraud, 4) physical loss of non-electronic records or portable devices lost, discarded, or stolen, 5) stationary devices lost, discarded, or stolen such as computers or servers not designed for mobility, and 6) insider breaches where someone such as an employee or contractor with legitimate access breaches information (PRCH, 2012). It is the latter insider category that is the focus of this study. The assumption is that this form of data breach would occur by organizational members or employees initiating such information sabotage acts within their own organization.

Giacalone and Knouse (1990) initially identified information sabotage acts as information tactics whose culprit would be difficult to identify and who also capitalized on company weaknesses such as spreading rumors, altering or deletion of data and placing of false orders. Hafer and Gresham (2009) defined organizational-based, information sabotage as malicious, purposeful and covert or overt attempts by employees to intentionally and with premeditation hinder, harm or prevent the acquisition, dissemination and response to marketing/customer/company information. Malicious intent was the defining factor separating sabotage from simple mistakes, negligence or errors. The harm from these malicious acts could come from damage to the company's image, reputation, or relationships with vendors or customers. Covert acts like misdirecting information could be seen as "soft demeanor" that might be tolerated as something everyone does once in a while. Destruction of computer files or stealing a work computer would be considered as unethical, purposefully destructive, and felonious. Nevertheless, these latter types of acts represent highly severe circumstances in which harm is occurring to others in varying degrees and therefore, would represent moral and unethical violations (Graham, Nosek, Haidt, Iger, Koleva, & Ditto, 2011; Haidt, 2007; Kish-Gephart, Harrision, & Treviño, 2010; Rai & Fiske, 2011). Within the management literature, only Hafer and Gresham have investigated managers' perceptions of the frequency of types of employee-perpetrated acts of information sabotage (2012) and intrinsic antecedents to information sabotage (2009).

The most comprehensive literature on information sabotage-related research has focused on data leakage, data hacking and insider threats (Hanker & Probst, 2011; Huth Chadwick, Claycomb, & You, 2013; McCormick, 2008; McGowan, Stephens, & Gruber, 2007; Predd, Pfleeger, Hunker, & Bulford, 2008; Silic & Back, 2014; Warkentin & Willison, 2009). In this literature, a variety of technical, social, and socio-technical approaches have been used to present different definitions and characteristics of people involved in hacking and the monitoring, auditing, and security systems related to these information sabotage-related behaviors (Huth et al., 2013). Additionally, these sabotage episodes call into question the ability of an organization's managers to provide adequate moral and safeguard control systems within an organization to deal with these acts.

Committing information sabotage acts is often considered as a form of organizational deviance or organizational misconduct and often rises to the level of an organizational crime (Mars, 2006). Subsequently, much computer crime legislation has been passed (Conley & Bryan, 1999; Nahrstadt, 2009). However, managers still have to make moral decisions about what to do about these acts once they have been committed. Do they have tolerance for some acts verses intolerance for other acts is a central question? In other words, are managers willing to accept, welcome, or endorse the behavior revealed in committing some of these acts or do they not accept, do not welcome, or do not endorse such behavior committed in other acts? This acceptance or non-acceptance decisional stance fits the neo-classical definition of tolerance/intolerance posited by Von Bergen, Bressler, and Collier (2012) and represents the tolerance focus of this study.

Given that committing information sabotage is a moral decision, it is now recognized that personality traits such as one's own ethical ideology and situational factors such as one's organizational workplace have considerable impact on such decisions (Dubinsky, Nataraajan, &

Huang, 2004; Peterson, 2002; Stewart, 2007). Ethical ideology (Fortsyth, 1980) represents a system of ethics used to make moral judgments and an organization's culture represents one of the crucial workplace situational factors for assessing a dimension of ethical ideology for an individual contemplating the handling and/or committing of information sabotage acts (Caruana, 2001; Knouse & Giacalone, 1992). Organizational culture provides the organizational reality within which morally and ethically relevant actions are discussed, judged, and sanctioned. Consequently, organizational culture can be an influence on how managers, as institutional cultural pilots, might handle acts of information sabotage. As previously mentioned, there is a paucity of academic research that exists on the range of managerial tolerance that managers have regarding insider information sabotage acts and the research is essentially devoid of the type of organization culture that might influence their attitudinal tolerance on such acts.

The purpose of this paper is to employ a mixed-method research design that first quantitatively evaluates managerial tolerance attitudes that managers hold toward insider information sabotage acts and then to qualitatively explore and hypothesize which type or types of organizational cultures might be used to support their tolerance attitudes using Dual Culture Theory. To achieve this dual purpose, the paper is organized in the following fashion. First, the two respective literatures on information sabotage and then Dual Culture Theory are presented. Following the two literature reviews is the quantitative methodology and results of a survey administered to managers that empirically accesses their attitudinal tolerance of such acts. Following that, Dual Culture Theory will be offered as a possible explanation for hypothesizing the different organizational cultures that might support potential different levels of managerial tolerance of such acts. Finally, a discussion is provided that considers how these hypothesized organizational cultural results might be used in confirmatory research in the future.

It is important to recognize that this study represents a mixed-methods research approach. In mixed-methods research, the researcher combines elements of qualitative and quantitative research approaches in which research questions drive the methods used in the study and set the boundaries around the research project (Venkatesh, Brown, & Sullivan, 2016). Mixed-method research questions are "questions that embed both a quantitative research question and a qualitative research question within the same question" (Onwuegbuzie & Leech, 2006, p. 483). Furthermore, mixed-methods designs should be used when researchers intend to holistically explain phenomenon that has fragmented, inconclusive, and/or equivocal extant research (Venkatesh et al., 2016). In this paper, the overall research question is asking whether managers hold differing levels of tolerance toward various insider information sabotage acts and what kind or kinds of organizational cultures might these managers use to support their tolerance perspectives. The first part of the question about what are managerial levels of tolerance can be addressed by quantitative methods. The second part of the question, since no research exists on the relationship, lends itself to qualitative methods research. This latter research design was judged most appropriate for this study because it attempts to eexplore what novel hypotheses and/or extensions of theoretical understanding might be generated from a previously unexplored situation.

Information Sabotage Literature

The general concept of employee sabotage has been discussed in industrial sociology, organizational behavior, industrial relations, and computer-related data leakage and insider threats literatures (e.g., Richards, 2008; Warkentin & Willison, 2009). The initial consideration of employee sabotage as a deviant workplace behavior was viewed as 'property deviance' which described the behavior in which workers illicitly acquired or damaged property or assets that belonged to their organization (Hollinger & Clark, 1982). This included sabotaging equipment, stealing company property, spreading rumors about coworkers/customers, and /or attempting to look busy while wasting time (Klotz & Buckley, 2013; Skarlicki & Folger, 1997; Skarlicki, van Jaarsveld, & Walker, 2008). Essentially, this form of employee sabotage falls into three categories: those behaviors whose object it is to destroy machinery or goods; those that stop production, and those that reduce the amount of work being done (Crino, 1994; Dubois, 1979; Giacalone & Knouse, 1990; Giacalone & Rosenfeld, 1987).

The advent of the Information Age shifted the focus on ways employees could go about harming their employment organizations. The focus on employee sabotage switched to 'behavior representing deviance or violations of the boundaries of workplace norms' that indicate minimum quality and quantity of output and expected efforts of employees (Hollinger & Clark, 1982) such as quota restrictions/goldbricking, social loafing, loafing in virtual teams, cyberloafing, and all kinds of computer hacking, espionage and sabotage (Klotz & Buckley, 2013).

Organizational Culture Introduction

One of the social and leadership factors often mentioned as a contributor to information sabotage behavior is the culture/environment (Appelbaum, Iaconi, & Matousek, 2006; Appelbaum, Shapiro, & Molson, 2007; Guzman & Stanton, 2009; Hunker & Probst, 2011; Leidner & Kayworth, 2006; Warkentin & Willison, 2009). Research on the context of the possible different organization cultures that enable information sabotage acts to occur has been relatively neglected except for the above mentioned data leakage and hacking literature (Guzman & Stanton, 2009; Leidner & Kayworth, 2006). Organizational culture research may also lend answers to a fundamental question as to why managers could be tolerant or intolerant of such acts (Huth et al., 2013; Richards, 2008; Warkentin & Willison, 2009).

Deal and Kennedy (1982) defined organizational culture as the "way things are done around here". Schein (1996) defined culture as a pattern of shared basic assumptions, values, norms and behaviors that were learned by the group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore taught to new members as the correct way to perceive, think, and feel in relation to those problems. An organization's culture is a social glue that serves as a sense-making and control mechanism that provides appropriate standards for guiding and shaping the attitudes and behaviors for what employees should say and do (Deal & Kennedy, 1983; O'Reilly & Chatman, 1996). It defines the rules of the game and is used to assess whether organizational members' attitudes and behaviors are compatible with the culture. What top management or organizational leadership says and how they behave sets the general climate of what is and is not acceptable moral and legal behavior in terms of organizational structure, compensation systems, customer

relations policies, human resource policies, and individual behavior and motivation (Gregory, Harris, Armenskies, & Shook, 2009; Niehoff, Enz, & Grover, 1990; Trice & Beyer, 1991).

Dual Culture Theory Literature

Dual Culture Theory or Grid/Group Cultural Theory is a theoretical framework to help identify what types of organizational cultures might govern the values, attitudes, and behaviors of managers that have to deal with various acts of information sabotage. The basic premise is that any community has several cultures and that each culture defines itself by contrast with the others. Dual Culture Theory had its beginnings in social anthropology of religion in primitive African tribes by Douglas (1970, 1973, 1996) and was further developed by Thompson and Wildavsky (1986). The bias for a particular culture is maintained by supporters who charge the other cultures with moral failure, thus, the theory presents four types of cultural bias that are at constant war with one another (Douglas, 1973, 1996; Thompson & Wildavsky, 1986).

This theory has been applied in different research domains like public administration (Hood, 1998), political science (Douglas & Mars, 2003; Jensen, 1998; Thompson, Ellis, & Wildavsky, 1990), organizational ethics (Loyens, 2013; Maesschalck, 2004; Mars, 1982; Patel & Schaefer, 2009), and project business organizations (Auch & Smyth, 2010; Roberts, Kelsey, Smyth, & Wilson, 2012). It has also been investigated in a variety of information-related concerns such as whistleblowing (Evans, 2008; Loyens, 2013), information bias (Thompson & Wildavsky, 1986), terrorism (Douglas & Mars, 2003) and sabotage/workplace crime (Mars, 1982, 2006), but not specifically on information-related sabotage.

Dual Culture Theory (Douglas, 1970, 1982) is both a theory and a typology and uses two social dimensions called ‘group’ and ‘grid’ to represent a matrix of four cultural patterns. The ‘group’ horizontal axis represents the extent to which people are restricted in thought and action by their strong or weak commitment to a group (Gross & Rayner, 1985; Hood, 1998). The greater the commitment (a high score) on this dimension, the more individual choice is weighted and subjected by group determination and the individual’s behavior is constrained by the group. A low score on this dimension (low group) means that people define themselves strongly as individuals and tend to act on their own behalf rather than that of a group. Consequently, their thinking, beliefs, values and actions are less strongly enabled and constrained by group norms and these people could consider themselves members of multiple groups and do not rely on just one single significant group for support and belonging. People in this group would tend to act in a more entrepreneurial, competitive manner, whereas, the high group score individuals are more deeply committed to a group and are less likely to compete with other group members and subsequently consider their action choices, values, beliefs and thoughts to be strongly circumscribed by group customs and traditions.

The ‘grid’ vertical axis refers to the extent to which an individual’s life is bounded and constrained by their role and status (externally imposed rules, prescriptions, and stratification) in the larger social system (Gross & Rayner, 1985). According to Mars (1982), a high grid score means that an individual’s thinking, values, and decision making will be prescribed by the social position they occupy and that social interactions tend to be based on position and hierarchy, rather than reciprocity with another individual. A low grid score means that an individual is less

constrained by social position, hierarchy and formally defined criteria and would be more focused on negotiations occurring between different parties concerned.

The resultant matrix of high versus low grid/group scores produces a matrix of four organization cultural forms: hierarchical (high grid, high group), egalitarianism (low grid, high group), individualism (low grid, low group), and fatalism (high grid, low group). These four organizational cultures are shown below in Figure 1 and follow the traditional format of being illustrated as a 2 x 2 matrix (Douglas, 1973, 1978; Loyens, 2013; Mamadouh, 1999). Furthermore, the matrix is intended to illustrate the identity of cultural pluralism, which means that an organization's culture contains many different cultures (Auch & Smith, 2010; Hendry, 1999; Roberts et al., 2012; Schein, 1996).

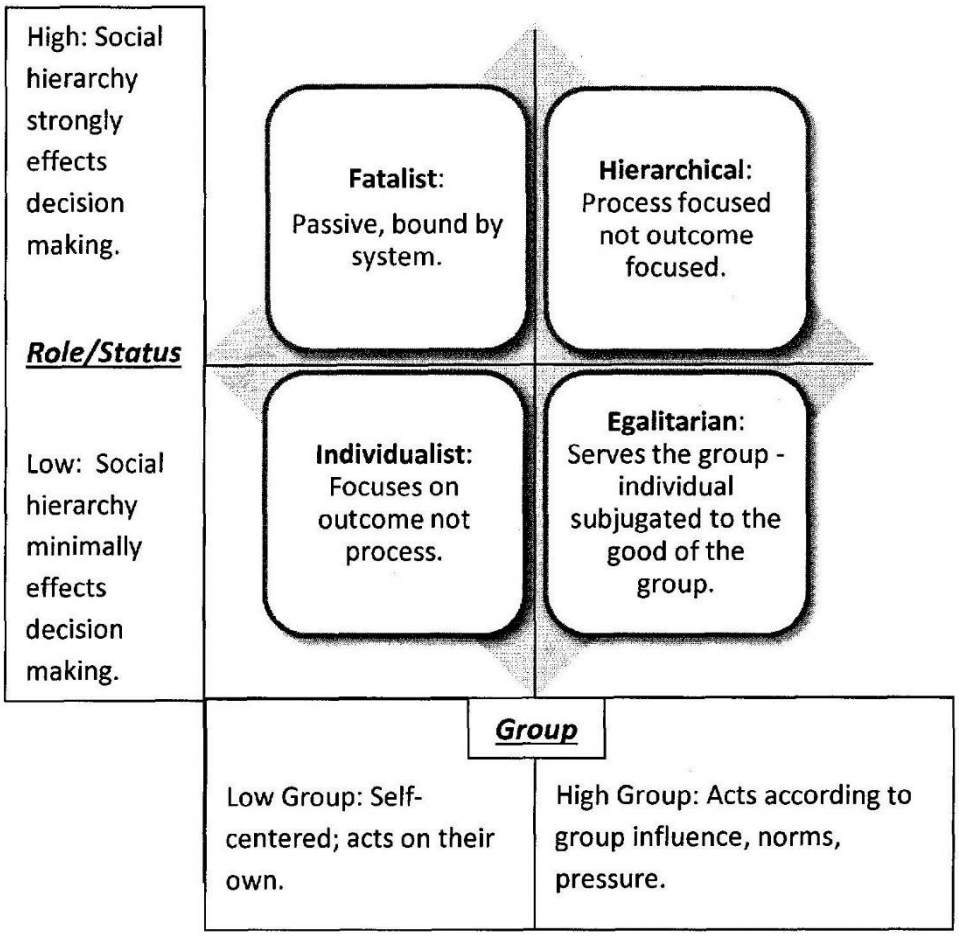

Figure 1. Four organizational cultures representing dual culture theory

In a "hierarchical culture", individuals know their place, but that place or position may evolve over time. This culture values security, performance and tolerance for set procedures and rules. It is intolerant to overt competition and allows only restricted and carefully controlled social mobility. However, both compulsion and inequality can be observed. This is a process-oriented culture that is more concerned with procedures and the properties of who does what

rather than with the outcomes of these processes and procedures (Hood, 1998; Loyens, 2013; Mamadouh, 1999; Mars, 2006; Patel & Schaefer, 2009).

The "individualistic culture" allows its members maximum opportunities for negotiating relationships and changing allegiances. Individuals tolerate spatial and social mobility and are valued for their actions and accomplishments. They do not appreciate or tolerate external constraints on their behavior and place few constraints on others. Self-regulation, mutuality, and respecting the rights of others are highly valued and tolerated in this culture. The focus here is on outcomes rather than process. This competitive solidarity is often associated with free market business organizations (Hood, 1998; Loyens, 2013; Mamadouh, 1999; Mars, 2006; Patel & Schaefer, 2009).

The central assumption of the "egalitarian culture" is that all individuals in the group are equal and decisions should be made collectively, possibly leading to the creation of informal rules. Deliberation and group negotiation are used in order to reach consensus. Group boundaries are set, which leads to distrust of outsiders and an us-versus-them attitude. Within this egalitarian sect, solidarity is highly valued and individual interests are subjugated to the welfare and higher good of the group or sect. Failure to serve the group interest is not tolerated (Hood, 1998; Loyens, 2013; Mamadouh, 1999; Mars, 2006; Patel & Schaefer, 2009).

The "fatalist culture", is a passive culture in which individuals feel bounded by a system of rules that is beyond their control and against which they cannot undertake collective action. Members are highly suspicious of others because they do not know what to expect from them. This fatalistic solidarity is characterized by small group, face-to-face interactions, participative decision making, a network of reciprocal exchanges, and few constraints on its members who are bound together by a high group consciousness and voluntary respect for the concern of others (e.g., Loyens, 2013; Patel & Schaefer, 2009). This culture emerges when individuals in a strong hierarchical structure have been excluded from decision making and subsequently, experience the social isolation of the individualistic members, but without its autonomy. They also experience the control typical of the hierarchical cultural members, but without the hierarchical group's support (e.g., Patel & Schaefer, 2009). This is a very unpredictable and estranged form of organizational life (Hood, 1998).

One final comment about Dual Culture Theory research deserves mentioning in order to understand the intentions behind this study. The anthropological measure of different cultures has few direct substantiated and validated quantitative measurement instruments. The interpretation of the respective cultures in Dual Culture Theory use utilizes qualitative rather than the more positivistic empirical quantitative methods. Van Maanen (1979) defined qualitative research as "an umbrella term" to cover "an array of interpretative techniques" that can describe, decode, translate, and otherwise come to terms with the meaning, not the frequency, of a certain more or less naturally occurring phenomena in the social world. The emergent inquiring perspective of this research focus is "truly in the moment," on the emergence of ideas, thoughts, feelings and how these develop, shape and are shaped by others (Keegan, 2009).

Method

Questionnaire Development and Measures

Nineteen acts of information sabotage were specifically identified for this study. These acts were modified from forms of sabotage originally published by Giacalone and Knouse (1990) and Richardson (2008). The final version of the questionnaire was also modified with input from security professionals from two companies in the location of the researchers.

The four questionnaire response foils reflect varying degrees of attitudinal tolerance toward these acts. "This offense is not worthy of any action" would be indicative of high tolerance (coded 1). Increased intolerance is reflected in the remaining three sequenced response foils of "Minor offense-warning is sufficient" (coded 2), "Moderate offense—disciplinary action required" (coded 3), and "Major offense—termination should result" (coded 4 to indicate highest intolerance). The questionnaire items are presented in Table 1.

Respondents and Data Collection

The respondents came from a list of MBA and EMBA students over the age of 30 who had identified themselves as "managers" in the alumni profile list supplied by the university alumni association. This list included 3,228 names. Each was sent a questionnaire via USPS with a letter explaining its purpose. A total of 467 usable questionnaires were returned for a response rate of 14.5%. Females accounted for 40.2% of the respondents, males accounted for 59.8%. Fifty-six percent of the respondents were in the 46-64 age bracket, 35% were less than 31 years old, and 9% were over 65 years old. Forty-two percent worked in companies with over 1,000 employees. Fifty-five percent managed five or fewer employees and 25% managed more than 15 employees.

Results

The data were analyzed with exploratory factor analysis. A principal component analysis using a Varimax rotation was conducted on the 19 acts of information sabotage. The number of respondents (n=467) exceeds the recommended ratio of 10 responses per variable (Hair, Black, Babin, & Andersen, 2009). The Kaiser-Meyer-Olkin (KMO) measure was .898, thus verifying that the sampling accuracy was strong for the analysis (Field, 2009). Barlett's test of sphericity $\chi^2(171) = 2949.64$, $p < .000$, indicated that the correlations between items were sufficiently large for the factor analysis. The Varimax rotation produced four factors as shown in Table 1 along with their factor loadings, eigenvalues, and percentage of variance after rotation. The total cumulative variance explained by the four factors was 57.8%.

Table 1.

Factor Loadings of Acts of Information Sabotage

Item		Factor 1	Factor 2	Factor 3	Factor 4
4.	Purposely delays transfer of information	.553	.052	.289	.481
7.	Purposely provides inaccurate information to the requestor	.668	.180	.204	.158
9.	Purposely misdirects information	.682	.069	.237	.291
10.	Purposely provides misinformation; either provides a better outlook or a worse outlook for a company.	.678	.266	.231	-.117
11.	Creates misinformation about a co-worker or manager	.774	.225	-.045	-.089
13.	Gathers information in a low and slow manner; collecting critical information unnoticed	.665	.142	.001	.321
14.	Holds information hostage, i.e., passwords to critical systems	.586	.354	-.052	.183
8	Steals proprietary information	-.016	.624	.137	.272
12.	Hijacks electronic communications to alter the content in an unfavorable manner for the sender of the information	.171	.673	.072	.242
15.	Alters or erases backup data making recovery impossible	.252	.765	.098	.062
16.	Alters system and application logs to cover up one's activities	.347	.677	.139	-.093
17.	Alters network routing to enable "man-in-the-middle" attacks and/or information capture	.311	.647	.193	.047
18.	Public release of proprietary data	.099	.647	.158	.236
1.	Maliciously alters files	.111	.178	.838	.050
2.	Malicious hacking	.018	.204	.812	.108
3.	Deliberately deletes files	.270	.117	.586	.271
5.	Physically damages software, hardware or a network	.075	.213	.144	.735
6.	Purposely alters security measures	.171	.387	.203	.422
19.	Takes critical systems or services off-line, a denial of service	.330	.435	.051	.487
Eigenvalues		3.612	3.500	2.128	1.745
Percentage of variance after rotation		19.012	18.419	11.200	9.182

Factors with eigenvalues greater than 1 were retained. Individual questions with loadings of .40 or above (Caro & Garcio, 2007; Comrey & Lee, 1992; Costello & Osborne, 2005; Elloy & Patil, 2014; Jabnoun & Khalifa, 2005), and those with cross loadings higher than .32 (Tabachnick & Fidell, 2001) were retained in the factor analysis. Reliability analysis for the acts comprising each of the four factors yielded Cronbach alphas of .84, .83, .69, and .58, respectively. Except for factor 4's alpha, the first three Cronbach alphas offer acceptable internal

reliability (Cronbach, 1951). The labeling of each factor was guided by the calculation of a grand mean score of the significant acts within each factor as indicated in Table 2 and also by a reasoned estimation of the amount of technical sophistication needed by a perpetrator to carry out the acts.

Table 2.

Grand Mean Score Descriptive Statistics

	N	Grand Mean	Std. Deviation	Std. Error
FACTOR 1	464	3.3560	.50120	.02327
FACTOR 2	463	3.8105	.34479	.01602
FACTOR 3	462	3.8777	.28797	.01340
FACTOR 4	462	3.8135	.33247	.01547

Each of the nineteen acts of information sabotage had an original mean score calculated from the results of all of the respondents. These original mean scores for each of the significant acts within each factor were then summed to provide the grand mean score for that factor. This grand mean factor score represents the aggregate responding manager's attitudinal value toward these acts using the scale of tolerance (coded 1) versus intolerance (coded 4). As shown in Table 2, the grand mean score of the seven positive loading acts of information sabotage comprising the first component factor was 3.36; 3.81 for the six positive loading acts comprising the second component factor; 3.88 for the three positive loading acts comprising the third component factor; and 3.81 for the three positive loading acts comprising the fourth component factor.

Paired t tests produced statistically significant differences between the grand mean score of factor 1 with factor 2 ($t(462 = -23.221, p < .001)$, factor 1 with factor 3 ($t(461) = -23.512, p < .001$), and factor 1 with factor 4 ($t(461) = -22.493, p < .001$). Also statistically different was factor 2's grand mean score from factor 3's score ($t(461) = -3.948, p < .001$) and factor 3's score from factor 4's score ($t(461) = 4.108, p < .001$). All four components factors reflected a characteristically high level of intolerance on the part of managers toward these acts of information sabotage.

The grand mean score on the manager's scale of tolerance-intolerance for Factor 1 is the lowest in intolerance, but widest in standard deviation compared to the other three factors. Factor 1 suggests that managers are not as intolerant as when other acts are evaluated for the other three factors. Furthermore, the standard deviation of this factor's grand mean score suggests that there was more diversity of opinion as to tolerance and managers seemed more conflicted as to whether factor 1 acts of information sabotage are worth doing anything about versus taking some sort of major HR action such as firing the saboteur.

Given the nature of the specific seven acts identified in Factor 1, it is reasonable to assume that a saboteur committing these acts would not require sophisticated knowledge of

information technology systems or operations in order to perform these acts. Many of the acts in Factor 1 could be considered as simple mistakes or errors. Thus, component Factor 1 was labeled *Purposeful Intolerant Manager, Little Technical Knowledge Saboteur*.

The component acts in Factor 2 moves dramatically toward greater managerial intolerance as these acts become more visible and more physically destructive. The six positive loaded acts include stealing, hijacking, altering or erasing, and releasing of proprietary data. The saboteur would need greater knowledge of information technology systems or operations in order to execute these acts. Consequently, component Factor 2 was labeled *Intolerant Manager, Average Technical Knowledge Saboteur*.

File manipulation across the three types of sabotage identified in Factor 3 generated the greatest amount of manager intolerance. Furthermore, the knowledge level of a saboteur's information technology systems or operations would need to be quite sophisticated in order to hack, alter, or delete system-wide files. Additionally, the standard deviation of the grand mean score for this factor was the smallest, thus, suggesting that managers had far less diversity of opinions about what to do about saboteurs committing these acts of information sabotage. Factor 3 was labeled *Extreme Intolerant Manager, Sophisticated Technical Knowledge Saboteur.*

Even though factor four suggests cautious interpretation because of low reliability and two acts having high cross loadings, the exploratory factor analysis did classify them as a factor and the technical nature of these three acts suggest they have face validity to represent creating the strongest information system-wide damage. The assumption of these three acts creating the most calamity seems further validated by suggesting that very high levels of professional knowledge of information technology systems or operations would be needed by a perpetrator in order to cause these acts. There was also a relative high level of managerial intolerance of and a low standard deviation across the three information sabotage acts loading in this factor. Factor 4 was labeled *Intolerant Manager, Professional and Highly Technical Knowledge Saboteur.*

Discussion of Quantitative-Method Results and Introduction of Qualitative-Method Hypotheses

The results suggest that managers are more intolerant as acts of information sabotage become more detrimental to the operation of their organization and as the anticipated level of saboteur's expertise needed to carry them out increases. As previously mentioned, Dual Culture Theory has usually been assessed via research in which novel hypothesis and/or extensions of theoretical understanding might be generated from a previously unexplored situation (Jaeger & Halliday, 1998). Attempts to relate types or patterns of organizational culture to specific acts of information sabotage have not received extensive research attention, but should gain momentum as organizations and saboteurs join the battle of wits to outperform each other.

Much of the early management research on organizational culture had a normative orientation in which culture was something to be managed. It was to be used as a tool to enhance organizational effectiveness and competitiveness and managerial values, norms, and behavior were to become the role model for others to follow in the organization's culture (Hatch & Cunliffe, 2013; Roberts et al., 2012). Trice (1993) suggests that an organization culture has two

major components: (1) substance or ideologies, which consists of shared systems of beliefs, values and norms; and (2) forms, which are observable ways or mechanisms such as common language and common ways of acting by members for expressing and affirming this cultural substance.

The previously determined factor analysis explored the tolerance-intolerance values of managers. Now the potential organizational cultural forms underlying these managerial values are assessed using Dual Culture Theory since culture has been deemed a critical variable needed to explain how social groups might interact with information technologies (Leidner & Kayworth, 2006). Based on the high intolerance values identified in Factors 2, 3, and 4, the "hierarchical culture" would seem rather obvious as the dominant organizational culture when managers interact with information technologies. Members in this type of organizational culture value order, discipline and control and they operate according to rules, value precedents, and respect rank. Any deviance to these group-set rules is controlled and infractions could be penalized (Loyens, 2013; Mars, 1982, 2006; Mamadouh, 1999; Patel & Schaefer, 2009; Thompson & Wildavsky, 1986). Clearly, this organizational cultural perspective stresses the importance of well-defined rules, extensive documented operating procedures, clear-cut, chain-of-command authority structures and highlights managers' responsibility to deal with organizational misconduct (Hood, 1998). Thus, the "hierarchical culture" would try to enforce the words and actions of top managers charged with the responsibility of creating and enforcing the organization's information sabotage culture.

Factor 1 may be subject to considering other organizational cultural interpretations. It must be remembered that the intolerance grand mean score for Factor 1 was the lowest of all four factors and yet, had the largest standard deviation and required the least amount of assumed technical knowledge to commit the seven different acts within that factor. The initial interpretation for Factor 1's seven acts implied that these acts might be construed as errors or mistakes. Managers may view these acts as not being harmful enough to warrant legal or otherwise complicated and time-demanding, "hard core" disciplinary action. A verbal and/or written warning or additional technical training to prevent future mistakes or errors may be all the time and effort the manager instigates as actions against these acts. The leadership style on the part of the manager may be more democratic and communal as the manager interacts with organizational members having committed these acts (Rosette & Tost, 2010).

Given the significant moderation in their intensity of intolerance, managers have shifted their values and behaviors on how to deal with potential saboteurs who might commit Factor 1 sabotage acts. Managers may still follow hierarchical rules, policies and procedures, but they are more 'lenient' and 'moderate' rather than 'strict' and 'hard core' in dealing with these potential saboteurs. Furthermore, this value moderation may juxtaposition managers into supporting and following other organizational cultures.

The possibility that managerial values regarding the acts loading in Factor 1 could be interpreted as another organizational culture pattern is the interesting aspect of this research using Dual Culture Theory. Another hypothesized interpretation is that managers for Factor 1 acts are part of an "egalitarian culture". Managers in this culture stress the importance of having

a healthy organizational and social life filled with rich mutual communications and one in which social equality among group members is paramount (Hood, 1998).

These are managers who are somewhat resistant to the normative organizational culture approach. They view culture as a management tool as being unrealistic about the potential to control employee value and norm interpretations and behaviors especially if many of the acts in the first factor represent simple mistakes or errors. They may, and often do, challenge the ethics of managerial control (Hatch & Conliffe, 2013; Hood, 1998) and they subsequently, desire to make changes in the organization's cultural interface with information technologies (Leidner & Kayworth, 2006).

Interpreting Factor 1's acts of information sabotage supporting an "egalitarian organization culture" could also be supported by additional research literatures. The literature on Gen Y or Millennials suggests that an egalitarian leadership/management style is best suited to this generation because they do not conform particularly well to a "hierarchial culture" (VanMeter, Grisaffe, Chonko, & Roberts, 2013). The 2008 World of Work Survey suggests that 42-78% of millennial workers engage in some form of unethical work practice. These adult workers prefer to work in groups and are heavily group oriented (Howe & Strauss, 2000; Serchuk, 2011). They are assertive, believe they are right, and think others, especially their managers, should be flexible and collaborative with them. The social and collaborative emphasis of both workers and managers from this generation (remember 35% of the managers responding to the survey was under 35 years of age and therefore, would fall into the millennial population) are supportive of an "egalitarian organizational culture" (VanMeter et al., 2013).

Further evidence that an "egalitarian organization culture" has some standing in our business organizations comes from what are our mainstream American cultural values. A study by Doran and Littrell (2012) found U.S.A. residents have great positive social consciousness reflected in high benevolence, universalism, and strong individual self-direction, but low power and achievement drive. These values subsequently indicate an "egalitarian national and societal culture". Jogulu (2010) found that Anglo-Western cultures preferred to have the role of a manager to be a coordinating role in which managers encourage direct disagreement and have more open discussion procedures to resolve problems and disputes. These are active characteristics of an "egalitarian culture".

A third hypothesized interpretative assessment of Factor 1's cultural distinction could be an "individualistic culture". Managers in this organization culture appreciate independence, autonomy and the freedom to enter transactions with others. Cultural boundaries are provisional and members see rules as being made to be circumvented, broken, or at least bent through negotiations. Thus, flexibility, adaptation, and individual flair are highly valued and this pattern is justified by the pursuit of personal rewards in a competitive environment. Networking and extending their networks, in order to demonstrate success, as well as constantly seeking out new and fashionable personal skills represent the tendency of these cultural members to focus on outcomes rather than processes (Loyens, 2013; Mamadouh, 1999; Mars, 2006; Patel & Schaefer, 2009). This individualistic perspective puts its faith in market systems, tort law remedies and individual entrepreneurship and competition to get ahead personally and organizationally (Hood, 1998).

Research literature offering support for this cultural pattern suggests that most organizations typically contain a primary and secondary culture (Roberts et al., 2012). Hendry (1999) and Mars (2006) have suggested that business organizations are dual culture organizations of hierarchial versus individualistic cultures and there is a shift to an individualistic culture away from the hierarchial culture in contemporary organizations. They contend this growth in individualism is occurring in the more technological complex countries and in organizations where the emphasis is on the entrepreneurial aspects of work and manager roles. These changing roles reflect the tendency to support rule bending, short-termism, calculated risk-taking, and the cultivation of ever shifting networks favoring the individual over the employer or other stakeholders (Hendry, 1999; Mars, 2006). These psychological/social changes are supposedly producing shifts from organizational hierarchy constraints to organizational member individualistic freedoms, from supporting long-term organization positions to supporting short-term individual interests, and supporting the short-term interests of some top managers who sacrifice the organization's long-term interests in order to increase their organization's short-term share prices and protect their bonuses by whatever means they can (Mars, 2006).

It is feasible to suggest that managers have a desire to move up the management hierarchy and their obtaining positive performance outcomes count as a main promotional evaluation factor. Consequently, a number of the Factor 1 acts of information sabotage, especially if considered initially as errors or mistakes, could be manipulated by managers in their favor. For example, delaying information transmitted until more information is gathered could help the manager produce beneficial decision making outcomes, or providing initial misinformation or purposely misdirecting information about the organization may help the manager's unit competitive situation, or gathering information in a slow manner is a common tactic to stall organizational change that the manager may not see as beneficial. The outcomes of these acts may prove beneficial for the manager and/or for the organizational unit's performance. Flexibility, adaptation, and individual flair are highly valued and this pattern is justified by the pursuit of personal rewards in a competitive environment. The "individualistic organizational culture" mainly focuses on outcomes rather than process (Hood, 1998; Loyens, 2013; Mamadouh, 1999; Mars, 2006; Patel & Shaefer, 2009).

In summary, trying to hypothesize which organizational culture indulges the managerial tolerance-intolerance values of the seven information sabotage acts loading in the first factor allows for three possible interesting hypothsized interpretations and could serve as a genesis for future research. The match of significant and consistent high levels of intolerant managerial attitudes across Factors 2-4 would seem to support the notion that "hierarchial cultures" fit the acts of information sabotage identified in those three factors.

Finally, there was not enough evidence from the questionnaire to suggest any of the managers could be placed in the "fatalistic culture". This was not entirely unexpected given the nature of the information sabotage topic. It is reasonable to expect that even the most benign acts of information sabotage would find little sympathy or tolerance from the managers who could be targets themselves or responsible for the losses the sabotage may inflict on the organization, its customers, or its competitors. The data from these responding managers suggest they are all relatively intolerant of most of the nineteen acts of information sabotage as measured by the four

tolerance-intolerance questionnaire foils. Furthermore, as the sabotage and saboteurs' behaviors to commit these information sabotage acts become more sophisticated, managers have less tolerance.

Limitations and Future Research

Limitations

One limitation in this study was some acts of information sabotage displaying high cross factor loadings. Although it would be ideal for each act to have only one significant loading on one factor, in practice, many of the variables in a factor structure will have several moderate sized significant loadings, which makes the job of interpreting the respective factors much more difficult (Gorsuch, 1983; Hair et al., 2009; Thompson, 2004). It should be underscored that numerous studies have used factor loadings of .40 or above for items cross loading in their factor analysis (Caro & Garcio, 2007; Comrey & Lee, 1992; Costello & Osborn, 2005; Elloy & Patil, 2014; Jabnoun & Khalif, 2005).

Future Research

Dual Culture Theory has proven much more powerful in exploratory, anthropological studies. It was used here because the investigation of possible multiple or pluralistic organizational cultures being related to information technologies and acts of information sabotage is an embryonic field of research investigation. Other typologies of organizational cultures exist in various literatures. The Schein model of organizational culture incorporates artifacts, espoused values, and basic underlying assumptions (1996), but does not help articulate types of cultural heterogeneity. Hofstede's model (2005) focuses primarily on comparing organizational cultures between nations in which background, different roles and factors of identity are addressed. Cameron and Quinn's (2006) competing values framework offers an analysis of cultural diversity, but it is designed for private sector firms seeking competitive advantage. The Dual Culture model is broader in conception, applicable to a broader array of social groups, teams and organizations. It is most comparable with Schein's model and the emphasis on values (Roberts et al., 2012). Future research could:

- investigate ways to utilize and integrate the quantitative survey measures found in the Schein model (1996), the competing values framework model (Cameron and Quinn, 2006) and the Organizational Culture Inventory (OCI) (Cooke & Lafferty, 1987) with the qualitative anthropological measurement approach in the Dual Culture Theory model.
- conduct confirmatory studies to see if "hierarchical culture" type is the dominant culture supporting organizational managers when it comes to their interface with information technologies and especially acts of information sabotage.
- specifically replicate the seven acts in Factor 1 and then conduct confirmatory studies to see if either of this study's hypothesized "hierarchial", "egalitarian", or "individualistic culture" is significant.
- conduct investigative or additional exploratory studies to see what organizational cultures might exist for victims, including outside constituencies, of information sabotage acts and/or for non-affected organizational members.

In the absence of more inclusive and generalizable confirmatory research results, there can be no clear answers to the major organizational culture hypotheses presented in this study. One primary question raised is 'has the traditional "hierarchial cultural values" of managers remained strongly intolerant of the unethical and potentially criminal and organizationally punishable behavior of insider information saboteurs across all acts of information sabotage or has a shift in organizational cultural values for managers occurred when dealing with the less devious and less physical malicious acts?'. The corollary question assuming a shift has occurred is 'has the shift of supporting this misconduct occurred in exchange for individual personal and organizational rewards (an indication of tolerating "individual cultural values") or has the shift occurred as a result of assimilating into organizations the "egalitarian cultural values" of our nation in general?' This is a question that has come to the forefront when President Obama commuted the 35-year sentence of insider saboteur Ms. Chelsea Manning on January 17, 2017 (Jarrett & Borger, 2017). Future research is needed to clarify the mixed picture of potential different organizational cultures that may be identified with various acts of information sabotage. Each organizational culture causes people to act in different ways and to hold different shades of attitudinal tolerance versus intolerance of organizational members and management who commit such acts. Having some transparency about these cultural values, norms and behaviors who commit these acts should be mutually beneficial to both organizational managers and members.

Conclusions

This study has employed an interpretative, mixed-research methodology dealing with a quantitative-method questionnaire taken by organizational managers tapping into the range of their attitudinal tolerance on nineteen different acts of information sabotage. Qualitative-method research was then employed using Dual Culture Theory to hypothesize what types of organizational cultures might be used to explain what managers might use to support their tolerance attitudes toward these nineteen different acts of information sabotage. Given the importance of information technologies and the subsequent increase in various types of information sabotage, qualitative research is expected to progress toward confirmatory, quantitative research protocols. Furthermore, there is limited research in the managerial literature on managers' attitudinal tolerance/intolerance of information sabotage. This study may have served to start additional research on these important issues.

References

Applebaum, S. H., Iaconi, G. D., & Matousek, A. (2007). Positive and negative deviant workplace behaviors: Causes, impact, and solutions. *Corporate Governance, 7*(5), 586-598.

Applebaum, S. H., Shapiro, B. T., & Molson, J. (2006). Diagnosis and remedies for deviant workplace behavior. *Journal of American Academy of Business, 9*(2), 14-20.

Auch, F., & Smyth, H. (2010). The cultural heterogeny of project firms and project teams. *International Journal of Managing Projects in Business, 3*(3), 443-461.

Bressler, M. S., & Bressler, L. (2015). Protecting your company's intellectual property assets from cyber-espionage. *Journal of Legal, Ethical and Regulatory Issues, 18*(1), 21-34.

Cameron, K. S., & Quinn, R. E. (2006). *Diagnosing and changing organizational culture: Based on the competing values framework.* San Francisco: Jossey-Bass.

Caro, L. M., & Garcia, J. A. M. (2007). Measuring perceived service quality in urgent transport service. *Journal of Retailing and Consumer Services, 14*(1), 60-72.
Caruana, A. (2001). Anomie and deviant behavior in marketing: Some preliminary evidence. *Journal of Managerial Psychology, 16*(5), 322-338.
Christian, J. S., & Ellis, A. P. J. (2014). The crucial role of turnover intentions in transforming moral disengagement into deviant behavior at work. *Journal of Business Ethics, 119*, 193-208.
Cohen, T. R., Panter, A. T., & Turan, N. (2013). Predicting counterproductive work behavior from guilt proneness. *Journal of Business Ethics, 114*, 45-53.
Cohen, T. R., Panter, A. T., Turan, N., & Morse, L. A. (2012). The WECT project: Workplace experiences and character traits (project information). http://WECTProject.org.
Comrey, A. L., & Lee, H. B. (1992). *A first course in factor analysis* (2nd ed.). Hillsdale, NJ: Lawrence Arlbaum Associates.
Conley, J. M., & Bryan, R. M. (1999). A survey of computer crime legislation in the United States. *Information & Communication Technology Law, 8*(1), 35-57.
Cooke, R., & Lafferty, J. (1987). *Organizational culture inventory (OCI)*. Plymouth, MI: Human Synergistics.
Costello, A. B., & Osborne, J. W. (2005). Exploring best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research, and Evaluation, 10*(7), 1-9.
Crino, M. D. (1994). Employee sabotage: A random or preventable phenomenon? *Journal of Managerial Issues, 6*(3), 311-330.
Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*, 297-334.
Deal, T., & Kennedy, A. A. (1982). *Corporate culture*. Reading, MA: Addison-Wesley.
Deal, T. E., & Kennedy, A. A. (1983). Culture: A new look through old lens. *Journal of Applied Behavioral Sciences, 19*(4), 501-510.
Doran, C. J., & Littrell, R. F. (2012). Measuring mainstream U.S. cultural values. *Journal of Business Ethics, 117*, 261-280.
Douglas, M. (1973). *Natural symbols: Explorations in cosmology* (2nd ed.). London, UK: Routledge and Kegan Paul.
Douglas, M. (1978). *Cultural bias*. Occasional Paper No. 34, Royal Anthropological Institute of Great Britain and Ireland.
Douglas, M. (1996). *Natural symbols: Explorations in cosmology* (3rd ed.). London, UK: Routledge.
Douglas, M. (1999). Four cultures: The evolution of parsimonious model. *GeoJournal, 47*, 411-415.
Douglas, M., & Mars, G. (2003). Terrorism: A positive feedback game. *Human Relations, 56*(7), 763-786.
Dubinsky, A. J., Nataraajan, R., & Huang, W. (2004). The influence of moral philosophy on retail salespeople's ethical perceptions. *Journal of Consumer Affairs, 38*(2), 297-319.
Dubois, P. (1979). *Sabotage in industry*. Harmondsworth, UK: Pelican.
Elloy, D. F., & Patil, V. (2014). Self-leadership and burnout: An exploratory study. *International Journal of Business and Social Science, 5*(9), 7-13.
Evans, A. J. (2008). Dealing with dissent: Whistleblowing, egalitarianism, and the republic of the firm. *Innovation: The European Journal of Social Science, 21*(3), 267-279.

Field, A. P. (2009). *Discovering statistics using SPSS (and sex and drugs and rock 'n roll)*. Thousand Oaks, CA: Sage Publication.
Forsyth, D. R. (1980). A taxonomy of ethical ideologies. *Journal of Personality and Social Psychology, 39*(1), 175-184.
Giacalone, R. A., & Knouse, S. B. (1990). Justifying wrongful employee behavior: The role of personality in organizational sabotage. *Journal of Business Ethics, 9*(1), 55-61.
Giacalone, R. A., & Rosenfeld, P. (1987). Reasons for employee sabotage in the workplace. *Journal of Business and Psychology, 1*(4), 367-378.
Gorsuch, R. L. (1983). *Factor analyses* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.
Graham, J., Nosek, B. A., Haidt, J., Iger, R., Koleva, S., & Ditto, P. (2011). Mapping the moral domain. *Journal of Personality and Social Psychology, 101*(2), 366-385.
Gregory, B. T., Harris, S. G., Armenskis, A. A., & Shook, C. L. (2009). Organizational culture and effectiveness: A study of values, attitudes, and organizational attitudes. *Journal of Business Research, 62,* 673-679.
Gross, J., & Rayner, S. (1985). *Measuring culture: A paradigm for the analysis of social organizations*. New York: Columbia Press.
Guzman, I. R., & Stanton, J. M. (2009). IT occupational culture: The cultural fit and commitment of new information technologists. *Information Technology & People, 22*(2), 157-187.
Hafer, J. C., & Gresham, G. G. (2012). Managers' and senior executives' perceptions of frequency and type of employee-perpetrated information sabotage and their attitudes toward it: The results of a pilot study. *Journal of Behavioral and Applied Management, 13*(3), 151-167.
Hafer, J. C., & Gresham, G. G. (2009). Possible explanations for information sabotage: Potential research models. *Journal of Management, Spirituality & Religion, 6*(3), 233-245.
Haidt, J. (2007). The new synthesis in moral psychology. *Science, 316*(5827), 998-1002.
Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice Hall.
Hastings, S. E., & Finegan, J. E. (2010). The role of ethical ideology in reactions to injustice. *Journal of Business Ethics, 100,* 689-703.
Hatch, M. J., & Cunliffe, A. L. (2013). *Organization theory: Modern, symbolic and postmodern perspectives*. Oxford, UK: Oxford University Press.
Hendry, J. (1999). Cultural theory and contemporary management organization. *Human Relations, 52*(5), 557-577.
Henle, C. A., Giacalone, R. A., & Jurkiewicz, C. L. (2005). The role of ethical ideology in workplace decisions. *Journal of Business Ethics, 56*(3), 219-230.
Hofstede, G. J. (2005). *Cultures and organizations, software of the mind: Intercultural cooperation and its importance to survival*. New York: McGraw-Hill.
Hollinger, R. C., & Clark, J. P. (1982). Formal and informal social controls of employee deviance. *Sociological Quarterly, 23*(3), 333-343.
Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime, 22*(2), 242-260.
Hood, C. (1998). *The art of the state. culture, rhetoric, and public management*. Oxford, UK: Clarendon Press.
Howe, N., & Strass, W. (2000). *Millennials rising: The next great generation*. New York: Random House.

Howley, D. (2015). *The biggest computer hack attacks of the last 5 years*. Retrieved from http://www.yahoo.com/tech/the-biggest-computer-hack-attacks-of-the-last-5-years-125449860474.html.

Hunker, J., & Probst, C. (2011). Insider and insider threats: An overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*(1), 4-27.

Hunter, D. Y., & Bandow, D. (2009). Abusive managers and variables impacting retaliation in organizations. *The Business Review, 12*(1), 32-38.

Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers, 15*, 1-4.

Jarrett, L., & Borger, G. (2017). *Obama commutes sentence of Chelsea Manning*. CNN Politics. com. Retrieved from http://www.cnn.com/2017/01/17/politics/chelsea-manning-sentence-commuted

Jabnoun, N., & Khalifa, A. (2005). A customized measure of service quality in the UAE. *Managing Service Quality, 15*(4), 374-388.

Jaeger, R. G., & Halliday, T. R. (1998). On confirmatory versus exploratory research. *Herpetologica*, *54*(Suppl), 564-566.

Jensen, L. (1998). Cultural theory and democratizing functional domains. The case of Danish housing. *Public Administration, 76*(1), 117-139.

Jogulu, U. D. (2010). Culturally-linked leadership styles. *Leadership & Organization Development Journal, 31*(8), 705-719.

Keegan, S. (2000). 'Emergent inquiry': A practitioner's reflections on the development of qualitative research. *Qualitative Market Research: An International Journal, 12*(2), 234-248.

Khan, A. K., Quratulain, S., & Crawshaw, J. R. (2013). The mediating role of discrete emotions in the relationship between injustice and counterproductive work behaviors: A study in Pakistan. *Journal of Business Psychology, 28*, 49-61.

Kish-Gephart, J. J., Harrison, D. A., & Treviño, L. K. (2010). Bad apples, bad cases, and bad barrels: Meta-analytic evidence about sources of unethical decisions at work. *Journal of Applied Psychology, 95*(1), 1-31.

Klotz, A. C., & Buckley, M. R. (2013). A Historical perspective of counterproductive work behavior targeting the organization. *Journal of Management History, 19*(1), 114-132.

Knouse, S. B., & Giacalone, R. A. (1992). Ethical decision-making in business: Behavioral issues and concerns. *Journal of Business Ethics, 11*(5/6), 369-377.

Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Towards a theory of it-culture conflict. *MIS Quarterly, 30*(2), 357-399.

Loyens, K. (2012). Towards a custom-made whistleblowing policy. Using grid-group cultural theory to match policy measures to different styles of peer reporting. *Journal of Business Ethics, 114*, 239-249.

Maesschalck, J. (2004). Approaches to ethics management in the public sector: A proposed extension of the compliance–integrity continuum. *Public Integrity, 7*(1), 21-41.

Mamadouh, V. (1999). Grid-group culture theory: An introduction. *GeoJournal, 47*(3), 395-409.

Mars, G. (2006). Changes in occupational deviance: Scams, fiddles and sabotage in the twenty-first century. *Crime Law Societal Change, 45*, 285-296.

Mars, G. (1982). *Cheats at work. An anthropology of workplace crime*. Aldershot, UK: Ashgate.

McCormick, M. (2008). Data theft: A prototypical insider threat. In S. Stolfo, S. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, & S. Smith (Eds.), *Insider attack and cyber security: Beyond the hacker* (pp. 52-67), New York: Springer.

McGowan, M. K., Stephens, P., & Gruber, D. (2007). An exploration of the ideologies of software intellectual property: The impact on ethical decision making. *Journal of Business Ethics, 73*, 409-424.

Nahrstadt, B. C. (2009). Former employee sabatoge? Invoke the Computer Fraud and Abuse Act. *Journal of Internet Law*, February, 17-26.

Niehoff, B. P., Enz, C. A., & Grover, R. A. (1990). The impact of top management actions on employee attitudes and perceptions. *Group and Organization Studies, 15*(3), 337-352.

Onwuegbuzie, A. J., & Leech, N. L. (2006). Linking research questions to mixed methods data analysis procedures. *The Qualitative Report*, *11*(3), 474-498.

O'Reilly, C. A., & Chatman, J. A. (1996). Culture as social control: Corporations, cults, and commitment. In B. M. Staw, & L. K. Cumings (Eds.), *Research in organizational behavior* (pp. 157-200). Greenwich, CT: JAI Press.

Patel, T., & Schaefer, A. (2009). Making sense of the diversity of ethical decision making in business: An illustration of the Indian context. *Journal of Business Ethics*, *90*(2), 171-186.

Peterson, D. K. (2002). Deviant workplace behavior and the organization's ethical climate. *Journal of Business and Psychology*, *17*(1), 47-61.

Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2008). Insiders behaving badly. *IEEE Security and Privacy*, *6*(4), 66-70.

Privacy Rights Clearinghouse (PRCH). (2012). *Chronology of data breaches*. Retrieved from http://www.privacyrights.org/data-breach

Rai, T. S., & Fiske, A. P. (2011). Moral psychology in relationship regulation: Moral motive for unity, hierarchy, equality, and proportionality. *Psychological Review, 118*(1), 57-75.

Richards, J. (2008). The many approaches to organizational misbehavior: A review, map and research agenda. *Employee Relations, 30*(6), 653-678.

Richardson, R. (2008). *2008 CSI computer crime & security survey*. San Francisco: Computer Security Institute.

Roberts, A., Kelsey, J., Smyth, H., & Wilson, A. (2012). Health and safety maturity in project business culture. *International Journal of Managing Projects in Business, 5*(4), 776-803.

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

Rosette, A., & Tost, L. (2010). Agentic women and communal leadership: How role prescriptions confer advantage to top women leaders. *Journal of Applied Psychology, 95*, 221-235.

Sanchez, J. I., Gomez, C., & Wated, G. (2008). A value-based framework for understanding managerial tolerance of bribery in Latin America. *Journal of Business Ethics*, *83*, 341-352.

Schein, E. (1996). *Organizational culture and leadership*. San Francisco: Jossey-Bass.

Serchuk, D. (2011, October 13). Move over baby boomers: The millennial generation has occupied wall street. *Forbes*.

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, *22*(3), 279-309.

Sinrod, E. J., & Reilly, W. P. (2000). Hacking your way to hard time: Application of computer crime laws to specific types of hacking attacks. *Journal of Internet Laws, 4*(3), 1-14.
Skarlicki, D. P., & Folger, R. (1997). Retaliation in the workplace: The roles of distributive, procedural and interactional justice. *Journal of Applied Psychology, 82*(3), 434-443.
Skarlicki, D. P., van Jaarsveld, D. D., & Walker, D. D. (2008). Getting even for customer mistreatment: The role of moral identity in the relationship between customer interpersonal injustice and employee sabotage. *Journal of Applied Psychology, 93*(6), 1335-1347.
Spreitzer, G. M., & Sonenshein, S. (2004). Toward the construct definition of positive deviance. *American Behavioral Scientist, 47*(6), 828-847.
Stewart, S. M. (2007). An integrated framework of workplace stress and aggression. *The Business Review, 8*, 223-233.
Tabachnick, B. G., & Fidell, L. S. (2001). *Using multivariate statistics* (5th ed.). Needham Heights, MA: Allyn and Bacon.
Tangney, J. P., Stuewig, J., & Mashek, D. J. (2007). Moral emotions and moral behavior. *Annual Review of Psychology, 58*, 345-372.
Thompson, B. (2004). *Exploratory and confirmatory factor analysis: Understanding concepts and applications*. Washington, DC: American Psychological Association.
Thompson, M., Ellis, R., & Wildavsky, A. (1990). *Cultural theory*. Boulder, CO: Westview Press.
Thompson, M., & Wildavsky, A. (1986). A cultural theory of information bias in organizations. *Journal of Management Studies, 23*(3), 273-286.
Trice, H. (1993). *Occupational subcultures in the workplace*. Ithaca, NY: ILR Press.
Trice, H. M., & Beyer, J. M. (1991). Cultural leadership in organizations. *Organization Science, 2*(2), 149-169.
VanMeter, R. A., Grisaffe, D. B., Chonko, L. B., & Roberts, J. A. (2013). Generation Y's ethical ideology and its potential workplace implications. *Journal of Business Ethics, 117*, 93-109.
Van Maanen, J. (1979). Reclaiming qualitative methods for organizational research: A preface. *Administrative Science Quarterly, 24*(4), 520-526.
Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems, 17*(7), 435-494.
Von Bergen, C. W., Bressler, M. S., & Collier, G. (2012). Creating a culture and climate of civility in a sea of intolerance. *Journal of Organizational Culture, Communications and Conflict, 16*(2), 85-104.
Wallace, E., de Chernatony, L., & Buil, I. (2011). Within-role, extra-role and anti-role behaviours in retail banking. *International Journal of Bank Marketing, 29*(6), 470-488.
Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*, 101-105.

