Implications of Student Perceptions Regarding the Disclosure of Sensitive Information

Marie A. Wright
Western Connecticut State University

Ronald G. Drozdenko
Western Connecticut State University

Information security breaches can be devastating to an organization, and in some cases, to the general public welfare. Because college students may be particularly susceptible to security breach influences, there are practical and ethical implications for understanding the likelihood that students would provide information to unauthorized entities. To that objective, a study was conducted that examined the conditions under which a security breach would be committed, the relationships between the respondent classification variables and the levels of acceptance of certain security breach situational factors, and the relationships between psychological well-being and religiosity, and the vulnerability to commit a security breach.

INTRODUCTION

The impact of security breaches caused by insiders significantly exceeds that caused by outsiders (Cappelli, Desai, Moore, Shimeall, Weaver, & Willke, 2007; Furnell & Phyo, 2003; Ponemon Institute LLC, 2012; Standage, 2002). The outcome of these security breaches can be devastating to an organization, and in some situations, to national security and the general public welfare. Thus, understanding the vulnerability of individuals to commit information security breaches has widespread practical and ethical implications.

College students may be particularly susceptible in situations where certain monetary, ideological, or personal incentives are provided. This is a notable concern. In 2010, 40% of full-time undergraduate students and 73% of part-time undergraduate students between the ages of sixteen and twenty-four were employed (National Center for Education Statistics, 2012). Among part-time college students who were employed, 33% of undergraduate students and 90% of graduate students worked at least thirty-five hours per week (National Center for Education Statistics, 2012). Unfortunately, there is no empirical research that helps to assess the risk that college students will commit an information security breach.

REVIEW OF THE LITERATURE

This literature review is not intended to offer an exhaustive investigation of all research related to security breaches, but rather to reference those studies from the organizational justice literature that address the motives for sabotage, where sabotage is defined as behavior that is intended to subvert,

disrupt, or damage an organization's operations, or cause harm to others (Crino, 1994). Sabotage can be directed at an entire organization, a particular unit, or a single individual (Giacalone, Riordan, & Rosenfeld, 1997). It also can have multiple targets (Ambrose, Seabright, & Schminke, 2002).

A number of studies have been done to identify possible motives for sabotage. Bennett (1998) and DiBattista (1991) found that individuals who experience feelings of powerlessness may engage in sabotage. Other research suggests that frustration can drive acts of sabotage (Chen & Spector, 1992; Spector, 1975; Storms & Spector, 1987; Taylor & Walton, 1971). The most frequently cited cause of sabotage, however, is injustice (Ambrose et al., 2002; Crino, 1994; Crino & Leap, 1989; DiBattista, 1989, 1996; Neuman & Baron, 1998; Robinson & Bennett, 1997; Sieh, 1987; Skarlicki & Folger, 1997; Tucker, 1993).

Three types of justice are differentiated in the organizational justice literature: Distributive justice refers to the perceived fairness of an outcome or reward allocation (Greenberg, 1990); procedural justice refers to the perceived fairness of processes or practices (Cropanzano & Greenberg, 1997); and interactional justice refers to the manner in which an individual is treated when procedures are enacted and outcomes are determined (Ambrose et al., 2002). Imbalances in distributive and procedural justice tend to be created by the organizational system, whereas inequities in interactional justice result from interactions with a particular person (Ambrose et al., 2002; Folger & Skarlicki, 1998; Greenberg, 1993).

While there has been debate about how these three forms of justice should best be assimilated into a general justice framework, there is clear agreement "that individuals respond not only to outcomes and procedures, but also to interpersonal interactions" (Ambrose et al., 2002). Furthermore, it has been shown that individual assessments of interactional justice are impacted by the information and explanations provided, and the interpersonal sensitivity conveyed (Ambrose et al., 2002; Folger & Skarlicki, 1998; Greenberg, 1993; Muzumdar, 2012).

Research suggests that when individuals engage in acts of sabotage in response to injustice, they do so in order to accomplish certain goals. DeMore, Fisher, and Baron (1988), Fisher and Baron (1982), and Sieh (1987), suggest that when perceptions of distributive injustice are the motivational force behind acts of sabotage, that the goal of these acts is to restore equity; to make up for an outcome that the individual felt was deserved but that was denied (Ambrose et al., 2002; Greenberg, 1996). Bies and Tripp (1998) and Bies, Tripp, and Kramer (1997) suggest that acts of sabotage might in fact have a different goal: revenge. In this case, the individual's retaliatory behavior is intended to cause harm to another, without regard to whether the retaliation improves the situation (Cropanzano & Baron, 1991; Greenberg, 1996; Neuman & Baron, 1997, p. 45). Studies suggest that perceptions of interactional injustice, and in particular, interpersonal insensitivity (e.g., harsh criticism or condescending treatment) play a significant role in retaliatory sabotage (Ambrose et al., 2002; Bies & Tripp, 1998; Folger & Skarlicki, 1998). Ambrose et al. (2002) found that perceptions of procedural injustice were equally associated with restoring equity and enacting revenge.

The literature suggests that individual responses to injustice tend to be directed toward the source of the perceived injustice. O'Leary-Kelly, Griffin, and Glew (1996) found that antagonistic behavior will be directed toward the target believed to be responsible for the negative outcome. Sheppard, Lewicki, and Minton (1992) suggest that individuals often feel the need to punish those responsible for treating them unfairly. Bennett (1998) suggests that when management's actions seem biased or their decisions appear inconsistent, employees will behave aggressively toward the person they feel is responsible.
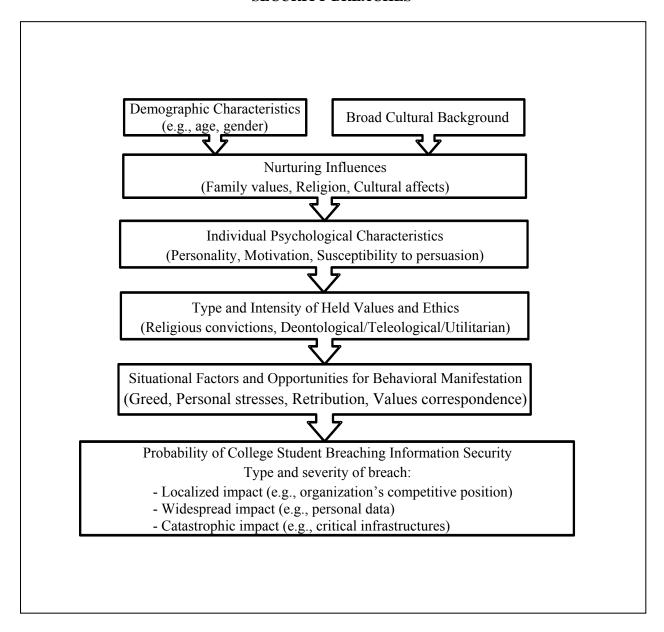
There appears to be an association between the level of perceived injustice and the severity of the response, although this relationship has not been explicitly examined in the literature. McLean Parks and Kidder (1994) found that distributive, procedural, and interactional injustice have an additive effect on the severity of sabotage. They suggest that there are behavioral changes that might occur as the level of perceived injustice increases. When a breaking point is reached, much like the straw that broke the camel's back, individual behaviors may become more dramatic. Ambrose et al. (2002) also found a cumulative effect between the different types of injustice (distributive, procedural, and interactional) and the severity of sabotage.

Although it is clear that those who engage in acts of sabotage do not do so on a random basis, and there are numerous studies that suggest that the victims of perceived injustice will direct their responses toward the source of the injustice in order to restore equity or enact revenge, we found no empirical research that helps to assess the susceptibility of students to varying situations where they might commit an act of sabotage, such as a breach in information security.

THEORETICAL FRAMEWORK AND RESEARCH QUESTIONS

Our working theoretical framework is presented in Figure 1.

FIGURE 1
WORKING CONCEPTUAL FRAMEWORK FOR SUSCEPTIBILITY TO INFORMATION SECURITY BREACHES

Based on the literature in the field, there are numerous factors that may contribute to the susceptibility of an individual to commit an information security breach. These include general demographics, cultural and sub-cultural backgrounds, individual psychological and ethical characteristics, and situational factors. Based on this framework, this study focused on three specific questions that were designed to assess the likelihood that undergraduate and graduate students in the U.S. would provide confidential information to unauthorized entities:

1) Under what conditions would a student commit a security breach?
2) Are there any respondent classification variables (e.g., gender, age, or other background) that are related to the levels of acceptance of certain security breach situational factors?
3) What are the relationships between college students' psychological well-being and religiosity, and their vulnerability to committing a security breach?

A nationwide study of undergraduate and graduate students was completed in September 2011. It evolved from our pilot study of undergraduate business students at Western Connecticut State University (Danbury, Connecticut), which was completed the previous year.

SURVEY INSTRUMENT

This research study utilized an anonymous three-part online survey for data collection. The first part of the survey consisted of a scenario in which a character was presented with an opportunity to provide information to an outside party who offered a monetary reward. Respondents rated the acceptability of the character to provide this information for each of thirty-one situations on a seven-point scale from "Absolutely Not Acceptable" to "Absolutely Acceptable." The situational factors, shown in Table 1, are original and were developed by us for the purpose of this study.

Two versions of the scenario were presented in random order to two random groups. The only difference between the versions concerned the amount of compensation received by the character for providing the information: One scenario provided compensation that was less than the character's weekly salary, while the other provided compensation that provided the character with financial security for life.

TABLE 1
SITUATIONAL FACTORS USED IN THE TWO SCENARIOS

1. Sam believes that the disclosure of the information could cause injury or death to other people.
2. The outside organization is a front for a radical group.
3. Sam believes that LBK is following dishonest practices, and deserves to be put out of business.
4. Sam believes that senior management at LBK is corrupt.
5. LBK is an energy company, and the outside organization wants information about LBK's nuclear power plant procedures.
6. LBK is a financial institution, and the outside organization wants information about LBK's electronic money transfer procedures.
7. Sam believes that the information that is disclosed will be used by the outside organization to gain a competitive advantage over LBK.
8. LBK managers have humiliated Sam in the presence of fellow employees on more than one occasion.
9. The outside organization is one of LBK's biggest competitors.
10. The outside organization is headquartered in the United States.
11. The outside organization is headquartered in another country.
12. Sam is a male who believes he is significantly underpaid by LBK.
13. Sam is a female who believes she is significantly underpaid by LBK.
14. Sam is a male who is satisfied with the income he earns at LBK.

15.	Sam has a sick parent who needs costly medical care, which Sam can't afford.
16.	Sam recently went through a divorce, and without the spouse's income, cannot afford to pay all of the bills.
17.	Sam believes that some employees at LBK are treated better than others, and that there are unequal opportunities for promotion.
18.	Sam believes in the values of the outside organization.
19.	Sam is sure that no one at LBK will ever find out how the outside organization acquired the information.
20.	Sam believes that it is possible, but unlikely, that anyone at LBK will ever find out how the outside organization acquired the information.
21.	Sam believes that someone at LBK will almost certainly find out how the outside organization acquired the information.
22.	Sam believes that the punishment for disclosing this information will be tolerable and mild.
23.	Sam recently applied for a job at the outside organization, and believes that providing the information will help to secure the position.
24.	LBK is a telecommunications company, and the outside organization wants information about LBK's equipment that handles emergency life safety services, such as 911 calls.
25.	LBK is an agricultural company, and the outside organization wants information about LBK's latest research in crop protection technology.
26.	The outside organization wants information that can be easily accessed from LBK's website.
27.	Sam believes that the information that is disclosed will be used by the outside organization solely for marketing purposes and will not jeopardize anyone's personal safety or security.
28.	Sam is a female who is satisfied with the income she earns at LBK.
29.	Sam believes that LBK is an honest and reputable company.
30.	Sam likes working at LBK and sees the potential for career advancement in the company.
31.	Sam believes that the punishment for disclosing this information will be harsh and severe.

Note: Respondents rated each situation on a 7-point scale from "Absolutely Not Acceptable" to "Absolutely Acceptable"

We chose to use a scenario-based approach, and to have the respondents indicate their level of acceptability for the character to provide information under different situational circumstances, rather than directly ask the respondents how they would react under different conditions. Studies in the social psychological literature suggest that scenarios provide a non-threatening method for responding to sensitive matters (Nagin & Pogarsky, 2001), and that individuals will answer more honestly if their responses are anonymous (Clark & Tifft, 1966; Hardt & Peterson-Hardt, 1977; Kulik, Stein, & Sarbin, 1968; Malvin & Moskowitz, 1983; Short & Nye, 1957-58; Wallerstein & Wyle, 1947).

In the second part of the survey, the respondents were asked to indicate their level of agreement with forty-five statements designed to measure psychological health. Forty of those statements are from the Ryff Scales of Psychological Well-Being (Ryff, 1989; Ryff & Keyes, 1995), a widely-used and validated instrument for measuring the six dimensions of psychological well-being: autonomy, environmental mastery, personal growth, positive relations with others, purpose in life, and self-acceptance. We received permission to use these scales in the study. The remaining five statements were written by us. The items in the second part of the survey are presented in Table 2.

TABLE 2
RYFF SCALES AND OTHER ITEMS RELATED TO PSYCHOLOGICAL HEALTH

Sometimes I change the way I act or think to be more like those around me.
I am not afraid to voice my opinions, even when they are in opposition to the opinions of most people.
My decisions are not usually influenced by what everyone else is doing.
I tend to worry about what other people think of me.
Being happy with myself is more important to me than having others approve of me.
I tend to be influenced by people with strong opinions.
People rarely talk me into doing things I don't want to do.
It is more important to me to "fit in" with others than to stand alone on my principles.
I have confidence in my opinions, even if they are contrary to the general consensus.
It's difficult for me to voice my own opinions on controversial matters.
I often change my mind about decisions if my friends or family disagree.
I am not the kind of person who gives in to social pressures to think or act in certain ways.
I am concerned about how other people evaluate the choices I have made in my life.
I judge myself by what I think is important, not by the values of what others think is important.
In general, I feel I am in charge of the situation in which I live.
The demands of everyday life often get me down.
I am quite good at managing the many responsibilities of my daily life.
I think it is important to have new experiences that challenge how you think about yourself and the world.
For me, life has been a continuous process of learning, changing, and growth.
I gave up trying to make big improvements or changes in my life a long time ago.
Maintaining close relationships has been difficult and frustrating for me.
People would describe me as a giving person, willing to share my time with others.
I have not experienced many warm and trusting relationships with others.
I live life one day at a time and don't really think about the future.
Some people wander aimlessly through life, but I am not one of them.
I sometimes feel as if I've done all there is to do in life.
When I look at the story of my life, I am pleased with how things have turned out.
In general, I feel confident and positive about myself.
I feel like many of the people I know have gotten more out of life than I have.
Given the opportunity, there are many things about myself that I would change.
I like most aspects of my personality.
I made some mistakes in the past, but I feel that all in all everything has worked out for the best.
In many ways, I feel disappointed about my achievements in life.
For the most part, I am proud of who I am and the life I lead.
I envy many people for the lives they lead.
My attitude about myself is probably not as positive as most people feel about themselves.
Many days I wake up feeling discouraged about how I have lived my life.
The past had its ups and downs, but in general, I wouldn't want to change it.
When I compare myself to friends and acquaintances, it makes me feel good about who I am.
Everyone has their weaknesses, but I seem to have more than my share.
I feel that I have been unjustly humiliated often by others.
Resolving difficult political conflicts with peaceful means is important to me.
My religious beliefs are very important to me.
Violent actions are acceptable to me if they are needed to advance my religious beliefs.
I would never accept the use of any action to support my religious beliefs that resulted in injury or death to other people.

Note: Respondents rated each item on a 6-point scale from "Strongly Disagree" to "Strongly Agree"

The last part of the survey contained general demographic questions to provide a more descriptive profile of the respondents.

SAMPLE

An e-mail was sent to faculty members who teach in the security programs at academic institutions whose information security courses are certified by the Committee on National Security Systems of the National Security Agency (National Security Agency, 2011a, 2011b). In total, 2,251 faculty at 158 colleges and universities in forty-one states received this e-mail, which explained the purpose of the research and requested their student participation in completing the online survey.

There were 741 responses, for an initial response rate of approximately 2.7%. Two hundred nineteen of those responses had missing data or were otherwise unusable and were discarded, leaving 522 usable responses (2% response rate). These response rates are estimated because exactly how many faculty involved their students in this research is unknown. We are confident that the rates are conservative estimates because they are based on the optimistic assumption that all 2,251 faculty encouraged their students to participate. Furthermore, because information security classes tend to be upper-level, technical courses with smaller enrollments, we realistically assumed an average class size of twelve students.

DEMOGRAPHIC CHARACTERISTICS

Sixty-six percent of the sample were males. The majority of the respondents were employed (25.0% full-time and 45.5% part-time), and 86.7% were single. Whites comprised 71.5% of the sample, Asians 11.0%, Hispanic or Latino 9.6%, and Black or African American 8.4%, with all other groups comprising less than 3% each. Most of the respondents were majoring in Information Systems/Information Technology (21.8%), Computer Science (21.0%), and Criminal Justice/Law (20.8%). Other academic majors included Management (7.9%), Engineering (7.1%), Accounting (4.7%), Marketing (4.5%), and Finance (3.9%), with all other majors comprising less than 2% each. The majority of the respondents were undergraduates (27.0% Seniors, 23.4% Juniors, 16.5% Sophomores, and 15.8% Freshmen). Approximately 17% were graduate students (13.3% Masters and 4.0% Doctorate). Eighty-nine percent of the respondents were U.S. citizens, with 26.7% having resided in another country for more than one month. The average age of the respondents was 24 years.

ANALYSIS AND RESULTS

All statistical analyses were computed using SPSS version 18.0. Non-parametric inferential statistics are primarily reported in order to be conservative in rejecting the null hypothesis, except as noted. For all of the following non-parametric analyses, analogous parametric statistics yielded similar results. Two-tail probability levels are reported.

There were an almost equal number of respondents to the two versions of the survey scenario: 264 students responded to the low pay scenario (i.e., the compensation was less than the character's weekly salary), and 258 students responded to the high pay scenario (i.e., the compensation provided the character with financial security for life).

Reliability Analysis

The ratings on the thirty-one situational factors were subjected to an analysis for internal consistency using Cronbach's alpha. Cronbach's alpha is generally regarded to indicate the extent to which a set of items measures a single uni-dimensional latent construct. The Cronbach's Alpha computed on the thirty-one situational factors was 0.960, indicating a high level of internal consistency. Other reliability statistics yielded similar results: the Spearman-Brown Coefficient was 0.939 and the Guttman Split-Half Coefficient was 0.930.

Research Question 1: Under what conditions would a student commit a security breach?
    This question considered the situational factors under which the character, Sam, might commit a security breach. Table 3 presents the situations ordered from least acceptable to most acceptable based on the grand mean of the sample. The Friedman Test Statistics indicated that there were statistically significant differences among the situational factors in this study (Chi-Square =9409.64, df=75, p<.001.) Paired comparisons of the situations were examined using Mann-Whitney U-tests and analogous Bonferroni adjustment for multiple comparisons. Statistically significant differences were found. Specifically, each of the top ten least acceptable situations was statistically significantly different at the 0.05 probability level from the bottom ten most acceptable situations.

    Research Question 1 also considered the level of monetary compensation for the breach. There were two experimental conditions in this study. One group rated the breach situations under the premise that the compensation for the information would be an amount of money that was less than the character's weekly salary. The other group rated the breach situations under the premise that the compensation for the information would be an amount of money that would make the character financially secure for life. In all thirty-one situations, the higher compensation yielded higher ratings of acceptability. A binomial sign test on the mean ratings yielded a two-tail probability of P<.0001. Independent sample Mann-Whitney U-tests were computed on each situation comparing the responses of the two payment groups. The results of these analyses are presented in Table 3.

TABLE 3
PAYMENT GROUP DIFFERENCES, MANN-WHITNEY U-TEST SIGNIFICANCE LEVELS

Situation	Mean	Z	Sig. (2-tailed)
Sam believes that the disclosure of the information could cause injury or death to other people.	1.96	-1.59	0.113
The outside organization is a front for a radical group.	2.00	-0.73	0.464
LBK is an energy company, and the outside organization wants information about LBK's nuclear power plant procedures.	2.06	-1.36	0.173
LBK is a financial institution, and the outside organization wants information about LBK's electronic money transfer procedures.	2.08	-2.02	0.043
Sam is sure that no one at LBK will ever find out how the outside organization acquired the information.	2.22	-2.14	0.032
The outside organization is one of LBK's biggest competitors.	2.23	-2.43	0.015
Sam believes that it is possible, but unlikely, that anyone at LBK will ever find out how the outside organization acquired the information.	2.26	-1.81	0.071
Sam believes that the punishment for disclosing this information will be tolerable and mild.	2.27	-2.14	0.032
The outside organization is headquartered in another country.	2.28	-2.30	0.022
Sam believes that the information that is disclosed will be used by the outside organization to gain a competitive advantage over LBK.	2.28	-2.78	0.006
LBK is an agricultural company, and the outside organization wants information about LBK's latest research in crop protection technology.	2.29	-0.93	0.351
Sam recently applied for a job at the outside organization, and believes that providing the information will help to secure the position.	2.40	-1.16	0.245
LBK managers have humiliated Sam in the presence of fellow employees on more than one occasion.	2.42	-1.72	0.086
Sam believes that someone at LBK will almost certainly find out how the outside organization acquired the information.	2.48	-0.69	0.488
Sam believes that some employees at LBK are treated better than others, and that there are unequal opportunities for promotion.	2.49	-2.27	0.023

Sam is a male who believes he is significantly underpaid by LBK.	2.52	-1.86	0.063
Sam recently went through a divorce, and without the spouse's income, cannot afford to pay all of the bills.	2.52	-1.30	0.192
Sam is a female who believes she is significantly underpaid by LBK.	2.62	-0.54	0.588
Sam believes that the information that is disclosed will be used by the outside organization solely for marketing purposes and will not jeopardize anyone's personal safety or security.	2.64	-1.82	0.069
LBK is a telecommunications company, and the outside organization wants information about LBK's equipment that handles emergency life safety services, such as 911 calls.	2.71	-0.07	0.944
Sam believes that the punishment for disclosing this information will be harsh and severe.	2.72	-1.12	0.261
Sam is a female who is satisfied with the income she earns at LBK.	2.76	-0.08	0.934
Sam is a male who is satisfied with the income he earns at LBK.	2.76	-0.48	0.633
Sam believes in the values of the outside organization.	2.77	-2.03	0.042
The outside organization is headquartered in the United States.	2.79	-0.50	0.616
Sam believes that senior management at LBK is corrupt.	2.88	-1.35	0.177
Sam has a sick parent who needs costly medical care, which Sam can't afford.	2.92	-2.86	0.004
Sam likes working at LBK and sees the potential for career advancement in the company.	2.95	-0.87	0.383
Sam believes that LBK is following dishonest practices, and deserves to be put out of business.	2.95	-1.39	0.164
Sam believes that LBK is an honest and reputable company.	3.02	-1.28	0.201
The outside organization wants information that can be easily accessed from LBK's website.	4.29	-0.62	0.537

Note: Situations are ordered from least acceptable to most acceptable based on the grand mean of the sample. The higher payment group rated each situation more acceptable.

Research Question 2: Are there any respondent classification variables (e.g., gender, age, or other background) that are related to the levels of acceptance of certain security breach situational factors?

Five respondent classification variables – gender, age, education level, marital status, and academic major – were found to be related to the level of acceptance of the security breach situational factors.

Gender

While there were no overall statistically significant differences between males and females in acceptability of information breaches, significant gender differences were found on the following specific situations at the 0.05 probability level using a Mann-Whitney U-test:

"Sam is a female who is satisfied with the income she earns at LBK." Females rated this breach more acceptable.

"Sam is a male who is satisfied with the income he earns at LBK." Females rated this breach more acceptable.

"Sam likes working at LBK and sees the potential for career advancement in the company." Females rated this breach more acceptable.

"LBK managers have humiliated Sam in the presence of fellow employees on more than one occasion." Females rated this breach less acceptable.

Age

Since age was examined as a continuous variable, Spearman Rho Correlations were computed. Age was found to be significantly negatively correlated to the composite acceptability score (i.e., sum of all situation acceptability ratings) and each of the individual situations at the 0.05 probability level. That is, as age increased, respondents rated the information security breach situations less acceptable. The Rho coefficient was 0.40 for the composite score and ranged from 0.12 to 0.36 for the individual situational factors.

Education Level

Level of education was also analyzed as a continuous variable. Using Spearman Rho Correlations, education level was found to be significantly negatively correlated related to the composite acceptability score and each of the individual situations at the 0.05 probability level. Similar to the findings with age, as educational level increased, respondents rated the information security breach situations less acceptable. The Rho coefficient was 0.34 for the composite score and ranged from 0.12 to 0.29 for the individual situational factors.

Marital Status

A Mann-Whitney U-test was computed to determine if there was a difference between married and single students in their overall acceptance of the situations. Using a composite score of all situations, single students rated the breach situations more acceptable than married students ($Z= -4.50$; $p<.001$). Further, for each of the thirty-one situations shown in Table 1, single students found them more acceptable than did the married students. For situational factors 2 through 27 in Table 1, this difference was statistically significant at the $p<0.05$ level.

Academic Major

A Mann-Whitney U-test was computed to determine if there was a difference between students in business majors and students in all other majors in their overall acceptance of the situations. Using a composite score of all situations, business students rated security breaches more acceptable than non-business majors ($Z= 4.248$; $p<.001$). Further, for each of the thirty-one situations shown in Table 1, business students found them more acceptable than did the students in other majors. For situational factors 9 through 31 in Table 1, this difference was statistically significant at the $p<0.05$ level.

Research Question 3: What are the relationships between college students' psychological well-being and religiosity, and their vulnerability to committing a security breach?

In order to reduce the probability of adding correlated variables into the model, a stepwise multiple regression (0.05 to enter; 0.10 to remove) was computed using the psychological well-being and religiosity items as independent variables and a composite acceptability score as the dependent variable. Nine variables were found to be statistically significant predictors of the overall acceptability of all breach situations. The overall R was .384 ($R^2=.15$) and the ANOVA on the model was $F=13.68$; $df=9/713$; $p<0.001$. The variance inflation factors for the final model were less than 1.50 for each included variable, indicating that multicollinearity is not a concern in the model. Standardized betas, t-values and p-levels for the individual items in the model are presented below.

The following four items in the model were negatively correlated with the acceptability composite score. In other words, the more respondents agreed with the statement, the less likely they were to accept a security breach.

"For me, life has been a continuous process of learning, changing, and growth." Standardized beta = -0.112; t=-2.87: $p<.004$.
"I am not the kind of person who gives in to social pressures to think or act in certain ways." Standardized beta = -0.127; t=-3.44: $p<.001$.
"I would never accept the use of any action to support my religious beliefs that resulted in injury or death to other people." Standardized beta = -0.079; t=-2.11: $p<.035$.

"My attitude about myself is probably not as positive as most people feel about themselves." Standardized beta = -0.076; t=-1.96: p<.050.

The following five items in the model were positively correlated with the acceptability composite score. In other words, the more respondents agreed with the statement, the more likely they were to accept a security breach.

"When I compare myself to friends and acquaintances, it makes me feel good about who I am." Standardized beta = 0.082; t=2.18: p<.030.

"I sometimes feel as if I've done all there is to do in life." Standardized beta = 0.099; t=2.52: p<.012.

"Violent actions are acceptable to me if they are needed to advance my religious beliefs." Standardized beta = 0.087; t=2.14: p<.033.

"I envy many people for the lives they lead." Standardized beta = 0.122; t=3.17: p<.002.

"I live life one day at a time and don't really think about the future." Standardized beta = 0.144; t=3.99: p<.001.

DISCUSSION OF THE RESEARCH RESULTS

There were differences in the perceived acceptability of committing an information security violation, depending on the situational factor and the amount of compensation offered. In addition, certain respondent classification variables were found to be related to the level of acceptance of the security breach situational factors, and specific variables related to psychological well-being and religiosity were found to be statistically significant predictors of the overall level of acceptability for committing a security breach. These findings are discussed in the following three sections.

Situational Factors

As shown in Table 3, the least acceptable situational factor is the belief that the disclosure of information could cause injury or death to other people. Although greater human risk seems to be associated with less acceptability, the high pay condition (i.e., compensation that provided the character with financial security for life) showed a decrease in the number of respondents who indicated that a situation was not acceptable. In fact, in every situation, there was greater acceptability of disclosing information if the payout was high. Simply put, money corrupts, and the higher the bribe, the more likely a security breach will occur. This finding is consistent with the criminal justice literature on the economics of crime (Becker, 1968; Bowles, 1997; Marselli & Vannini, 1997).

Committing a security breach was perceived to be most acceptable when the outside entity wants information that can be easily accessed from the organization's website. More than 72% of the respondents in both payment levels (i.e., compensation that was less than the character's weekly salary, and compensation that provided the character with financial security for life) felt it was highly acceptable to disclose information in this circumstance. For the purpose of this research study, this particular situational factor acts as validity test; since the information is publicly available, it should be more acceptable to give it away.

As shown in Table 3, this last situation, with a mean of 4.29 on a seven-point scale, was the only situation that was perceived to be acceptable to commit a security breach. In all other situations, the respondents felt it was unacceptable to commit a security breach. While such an ethical outcome is encouraging, there may be another explanation for this result: the respondents may be providing socially appropriate answers. This phenomenon, known as social desirability bias, causes the data to be analytically skewed toward the respondents' perceptions of what is "right" (Fisher, 1993). In this study, the respondents may have believed that the right answers were those in which the character did not provide information to the outside party. The effects of social desirability bias are believed to be mitigated through the use of indirect questioning (Robertson & Joselyn, 1974). Although our survey

employed the use of scenarios, with the respondents rating the situational factors from the perspective of the character in the scenario (i.e., indirect questioning), further empirical verification is needed.

Respondent Classification Variables

Five respondent classification variables were found to be related to the level of acceptance of the security breach situational factors.

Gender

Males and females were generally consistent in their perceptions of the acceptability of the situations; however, males were significantly less likely than females to find a breach acceptable when the salary earned was perceived to be satisfactory, and the company offered opportunities for career advancement. According to the U.S. Department of Commerce, Economics and Statistics Administration, and the Executive Office of the President, Office of Management and Budget (2011), "women are more likely to commit crimes now than in the past, although women who commit crimes are more likely to be arrested for nonviolent property crimes compared to male criminals whose crimes are more likely to involve violence."

Males were significantly more likely than females to find a breach acceptable when public employee humiliation was involved. This is a particularly interesting finding. Research conducted on the impact of humiliation suggests that it shares a psychological connection to terrorism (Marton, 2005; Morgan, 1989; Stern, 2003). The majority of terrorists are males, and studies suggest that their violent acts may be a direct outcome of the rage that results from having endured humiliating experiences (Marton, 2005).

Age

There was a negative correlation between age and the perceived acceptability of a security breach. This indicates that as respondents age, they tend to find all information security breach situations less acceptable. This finding is consistent with the curvilinear association between age and crime that has been well established in criminology: that "involvement in criminal behavior rises throughout the teenage years until it levels off during the late teenage and early adult years and then declines throughout the remainder of the life span" (Brame & Piquero, 2003).

Level of Education

There was a negative correlation between level of education and the perceived acceptability of a security breach. This indicates that as the respondents' educational level advances, they tend to find all information security breach situations less acceptable. This is consistent with research findings in criminology, which suggest that increasing education levels are associated with lower crime rates (Lochner & Moretti, 2004; Machin, Marie, & Vujić, 2011; Steurer, Smith, & Tracy, 2001).

Marital Status

Overall, married students rated the breach situations less acceptable than did single students. This finding is consistent with other studies, which suggest that people who are married may behave more responsibly than those who are not. For example, research conducted by McGee (2012) suggests that married people are more opposed to tax evasion than those who are single.

Academic Major

Students majoring in business found all security breach situations more acceptable than did non-business students. This is consistent with other research studies, which have found that business students exhibit lower ethical values than those in other academic majors (Goodman & Crawford, 1974; Hawkins & Cocanougher, 1972; McCabe, Dukerich, & Dutton, 1994; Newstrom & Ruch, 1976; Shuptrine, 1979).

Psychological Well-Being and Religiosity

Nine variables related to psychological health were found to be statistically significant predictors of the students' overall level of acceptability for committing a security breach. Four of those variables were negatively correlated:

> "For me, life has been a continuous process of learning, changing, and growth." Respondents who indicated a high level of agreement with this item were more likely to have a sense of continued development and personal growth (Ryff, 1989; Ryff & Keyes, 1995), and were less likely to find a security breach acceptable.

> "I am not the kind of person who gives in to social pressures to think or act in certain ways." Respondents who indicated a high level of agreement with this item were more likely to have a sense of independence, self-determination, and autonomy (Ryff, 1989; Ryff & Keyes, 1995), and were less likely to find a security breach acceptable.

> "I would never accept the use of any action to support my religious beliefs that resulted in injury or death to other people." Those who indicated a high level of agreement with this statement were less likely to find a security breach acceptable. This reinforces the situational factor that was found to be least acceptable (Table 3): the belief that the disclosure of information could cause injury or death to other people.

> "My attitude about myself is probably not as positive as most people feel about themselves." Respondents who indicated a high level of agreement with this item were more likely to have a low level of self-acceptance (Ryff, 1989; Ryff & Keyes, 1995), and were less likely to find a security breach acceptable.

Five variables that were found to be statistically significant predictors of security breach acceptability were positively correlated:

> "When I compare myself to friends and acquaintances, it makes me feel good about who I am." Respondents who indicated a high level of agreement with this item were more likely to have a high level of self-esteem (Ryff, 1989; Ryff & Keyes, 1995), and were more likely to find a security breach acceptable.

> "I envy many people for the lives they lead." On the surface, it would appear that this item contradicts the previous one. This statement, and the two previous items, are measures of self-acceptance on the Ryff Scales of Psychological Well-Being (Ryff, 1989; Ryff & Keyes, 1995); however, this item suggests that those with greater levels of personal dissatisfaction are more likely to find a security breach acceptable. The criminal justice literature helps to address this apparent contradiction. There are studies that suggest that non-violent criminals tend to have low self-images (Higgins, 1987; Little & Robinson, 1988, 2006; Luna, 1998; Wolfer & Roberts, 2008), while violent criminals tend to have high levels of self-esteem (Baumeister, Bushman, & Campbell, 2000; Baumeister, Smart, & Boden, 1996; Bushman & Baumeister, 2002; Gillespie, 2005; Kirkpatrick, Waugh, Valencia, & Webster, 2002; Ruiz, Smith, & Rhodewalt, 2001; Salmivalli, 2001; Twenge & Campbell, 2003).

> "Violent actions are acceptable to me if they are needed to advance my religious beliefs." The more respondents agreed with this item, the greater their ability to justify their actions, and the more likely they were to find a security breach acceptable.

> "I sometimes feel as if I've done all there is to do in life." Respondents who indicated a high level of agreement with this item were more likely to lack a sense of meaning or direction in life (Ryff, 1989; Ryff & Keyes, 1995), and were more likely to find a security breach acceptable.

> "I live life one day at a time and don't really think about the future." This item is similar to the previous one. Respondents who indicated a high level of agreement with this item were more likely to lack a sense of purpose in life (Ryff, 1989; Ryff & Keyes, 1995), and were more likely to find a security breach acceptable.

CONCLUSION

The results of this study suggest that there are situations under which students will more likely commit a security breach. The least acceptable situation is the belief that the disclosure of information could cause injury or death to other people, and the most acceptable situation is when the outside entity wants information that can be easily accessed from the organization's website. Regardless of the situation, there is a greater likelihood that a breach will be committed if the payout is high.

The results also indicate that a student's gender, age, level of education, marital status, and academic major may be related to the level of acceptance of certain security breach situations. Specifically, females may be more likely than males to find a security breach acceptable in spite of perceived income satisfaction and career advancement opportunities. Males may be more likely than females to find a breach acceptable when humiliation was experienced. Both males and females tended to find all information security breach situations less acceptable as they aged, and as their level of education advanced. Respondents who were single rated the breach situations more acceptable than did those who were married, and those majoring in business found all security breach situations more acceptable than did those majoring in a non-business discipline.

This study also found a relationship between the respondents' psychological well-being and religiosity, and their propensity to find information security breaches acceptable. Those respondents who were less likely to find a security breach acceptable tended to have a sense of continued personal development and growth, feelings of independence and autonomy, a low level of self-acceptance, and a strong belief that it was wrong to engage in any action that resulted in injury or death to others. Those respondents who were more likely to find a security breach acceptable tended to have a high level of self-esteem but envied others for the lives they led. They also tended to lack a sense of personal direction and purpose in life, and perceived violence to be acceptable if it was necessary to advance their religious beliefs.

The study reported here contributes to our understanding of the likelihood that students may commit an information security breach. Because this is the first empirical research conducted on this topic, further studies are needed to better understand the respondents' perspectives in interpreting the situational factors, to assess whether the effects of social desirability bias were effectively mitigated, to explore additional relationships between respondent classification variables and the level of acceptance of security breach situations, and to investigate whether other psychological health variables are statistically significant predictors of the students' overall level of acceptability for committing a security breach.

ACKNOWLEDGMENT

REFERENCES

Ambrose, M. L., Seabright, M. A., & Schminke, M. (2002). Sabotage in the workplace: The role of organizational injustice. *Organizational Behavior and Human Decision Processes*, 89, 947-965.

Baumeister, R. F., Bushman, B. J., & Campbell, W. K. (2000). Self-esteem, narcissism, and aggression: Does violence result from low self-esteem or from threatened egoism? *Current Directions in Psychological Science*, 9(1), 26-29.

Baumeister, R. F., Smart, L., & Boden, J. M. (1996). Relation of threatened egoism to violence and aggression: The dark side of self-esteem. *Psychological Review*, 103(V), 5-33.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76, 1169-1217.

Bennett, R. J. (1998). Perceived powerlessness as a cause of employee deviance. In R. W. Griffin, A. O'Leary-Kelly, & J. M. Collins (Eds.), *Dysfunctional behavior in organizations, Part A: Violent and deviant behavior* (pp. 221-240). Stamford, CT: JAI Press.

Bies, R. J., & Tripp, T. M. (1998). Revenge in organizations: The good, the bad, and the ugly. In R. W. Griffin, A. O'Leary-Kelly, & J. M. Collins (Eds.), *Dysfunctional behavior in organizations, Part B: Nonviolent dysfunctional behavior* (pp. 49-68). Stamford, CT: JAI Press.

Bies, R. J., Tripp, T. M., & Kramer, R. M. (1997). At the breaking point: Cognitive and social dynamics of revenge in organizations. In R. Giacalone, and J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 18-36). London: Sage.

Bowles, R. (1997). Casual police corruption and the economics of crime. *International Review of Law and Economics*, 17(1), 75-87.

Brame, R., & Piquero, A. R. (2003). Selective attrition and the age-crime relationship. *Journal of Quantitative Criminology*, 19(2), 107-127.

Bushman, B. J., & Baumeister, R. F. (2002). Does self-love or self-hate lead to violence? *Journal of Research in Personality*, 36, 543-545.

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., & Willke, B. J.. (2007). Management and education of the risk of insider threat (MERIT): Mitigating the risk of sabotage to employers' information, systems, or networks. Retrieved May 1, 2012, from http://www.sei.cmu.edu/reports/06tn041.pdf

Chen, P. Y., & Spector, P. E. (1992). Relationships of work stressors with aggression, withdrawal, theft and substance use: An exploratory study. *Journal of Occupational and Organizational Psychology*, 65, 177-184.

Clark, J. P., & Tifft, L. L. (1966). Polygraph and interview validation of self-reported deviant behavior. *American Sociological Review*, 31(4), 516-523.

Crino, M. D. (1994). Employee sabotage: A random or preventable phenomenon? *Journal of Managerial Issues*, 6, 311–330.

Crino, M. D., & Leap, T. L. (1989). What HR managers must know about employee sabotage. *Personnel*, 31-38.

Cropanzano, R., & Baron, R. (1991). Injustice and organizational conflict: The moderating effect of power restoration. *International Journal of Conflict Management*, 2, 5-26.

Cropanzano, R., & Greenberg, J. (1997). Progress in organizational justice: Tunneling through the maze. In L. T. Robertson, & C. L. Cooper (Eds.), *International review of industrial and organizational psychology* (pp. 317-372). New York, NY: John Wiley & Sons.

DeMore, S. W., Fisher, J. D., & Baron, R. M. (1988). The equity-control model as a predictor of vandalism among college students. *Journal of Applied Social Psychology*, 18, 80-91.

DiBattista, R. A. (1989). Designing a program to manage the risk of sabotage. *Supervision*, 6-8.

DiBattista, R. A. (1991). Creating new approaches to recognize and deter sabotage. *Public Personnel Management*, 20, 347-352.

DiBattista, R. A. (1996). Forecasting sabotage events in the workplace. *Public Personnel Management*, 25, 41-52.

Fisher, J. D., & Baron, R. M. (1982). An equity-based model of vandalism. *Population and Environment*, 5, 182-200.

Fisher, R. (1993). Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research*, 20(2), 303-315.

Folger, R., & Skarlicki, D. P. (1998). A popcorn metaphor for employee aggression. In R. W. Griffin, A. O'Leary-Kelly, & J. M. Collins (Eds.), *Dysfunctional behavior in organizations, Part A: Violent and deviant behavior* (pp. 43-82). Stamford, CT: JAI Press.

Furnell, S. M., & Phyo, A. H. (2003). Considering the problem of insider IT misuse. *Australian Journal of Information Systems*, 10(2), 134-138.

Giacalone, R. A., Riordan, C. A., & Rosenfeld, P. (1997). Employee sabotage: Toward a practitioner-scholar understanding. In A. G. Robert, & J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 109-129). Thousand Oaks, CA: Sage.

Gillespie, W. (2005). Racial differences in violence and self-esteem among prison inmates. *American Journal of Criminal Justice*, 29(2), 161-185.

Goodman, C. S., & Crawford, G. M. (1974). Young executives: A source of new ethics? *Personnel Journal*, 180-187.

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

Greenberg, J. (1993). The social side of fairness: Interpersonal and informational classes of organizational justice. In R. Cropanzano (Ed.), *Justice in the workplace: Approaching fairness in human resource management* (pp. 79-103). Hillsdale, NJ: Erlbaum.

Greenberg, J. (1996). What motivates employee theft? An experimental test of two explanations. Paper presented at the annual meeting of the Society for Industrial-Organizational Psychology, San Diego, CA (April).

Hardt, R. H., & Peterson-Hardt, S. (1977). On determining the quality of the delinquency self-report method. *Journal of Research in Crime and Delinquency*, 14(2), 247-261.

Hawkins, D. I., & Cocanougher, A. B. (1972). Student evaluations of the ethics of marketing practices: The role of marketing education. *Journal of Marketing*, 36, 61-64.

Higgins, E. T. (1987). Self-discrepancy: A theory relating self and affect. *Psychological Review*, 94, 319-340.

Kirkpatrick, L. A., Waugh, C. E., Valencia, A., & Webster, G. D. (2002). The functional domain specificity of self-esteem and the differential prediction of aggression. *Journal of Personality and Social Psychology*, 82(5), 756-767.

Kulik, J. A., Stein, K. B., & Sarbin, T. R. (1968). Disclosure of delinquent behavior under conditions of anonymity and nonanonymity. *Journal of Consulting and Clinical Psychology*, 32(5), 506-509.

Little, G. L., & Robinson, K. D. (1988). Moral reconation therapy: A systematic step-by-step. *Psychological Reports*, 62(1), 135-151.

Little, G. L., & Robinson, K. D. (2006). Recidivism outcome research on Moral Reconation Therapy in prisons-based therapeutic communities: A comprehensive review. *Cognitive-Behavioral Treatment Review*, 15(2), 14-17.

Lochner, L., & Moretti, E. (2004). The effect of education on crime: Evidence from prison inmates, arrests, and self-reports. *American Economic Review*, 94, 155-189.

Luna, R. (1998). In the mind of a criminal. *American Journal of Criminal Law*, 25(2), 479-484.

Machin, S., Marie, O., & Vujić, S. (2011). The crime reducing effect of education. *The Economic Journal*, 121(552), 463-484.

Malvin, J. H., & Moskowitz, J. M. (1983). Anonymous versus identifiable self-reports of adolescent drug attitudes, intentions, and use. *The Public Opinion Quarterly*, 47(4), 557-566.

Marselli, R., & Vannini, M. (1997). Estimating a crime equation in the presence of organised crime: Evidence from Italy. *International Review of Law and Economics*, 17, 89-113.

Marton, M. H. (2005). Terrorism and humiliation. Retrieved February 4, 2011, from http://www.humiliationstudies.org/documents/MartonBerlin05meeting1.pdf

McCabe, D. L., Dukerich, J. M., & Dutton, J. E. (1994). The effects of professional education on values and the resolution of ethical dilemmas: Business school vs. law school students. *Journal of Business Ethics*, 13(9), 693-700.

McGee, R. W. (2012). Marital status and the ethics of tax evasion. In R. W. McGee (Ed.), *The Ethics of Tax Evasion: Perspectives in Theory and Practice* (pp. 475-484). New York, NY: Springer.

McLean Parks, J., & Kidder, D. L. (1994). "Till death do us part...": Changing work relationships in the 1990s. In C. L. Cooper, & D. M. Rousseau (Eds.), *Trends in organizational behavior, Vol. 1* (pp. 111-136). London: Wiley & Sons.

Morgan, R. (1989). *The demon lover: The roots of terrorism*. New York, NY: Washington Square Press.

Muzumdar, P. (2012). Influence of interactional justice on the turnover behavioral decision in an organization. Retrieved April 4, 2012, from http://www.aabri.com/manuscripts/111019.pdf

Nagin, D. S., & Pogarsky, G. (2001). Integrating celebrity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence. *Criminology*, 39(4), 865-891.

National Center for Education Statistics. (2012). College student employment. Retrieved July 24, 2012, from http://nces.ed.gov/programs/coe/indicator_csw.asp

National Security Agency. (2011a). IA courseware evaluation program. Retrieved January 5, 2011, from http://www.nsa.gov/ia/academic_outreach/iace_program/index.shtml

National Security Agency. (2011b). IA courseware institutions. Retrieved January 5, 2011, from http://www.nsa.gov/ia/academic_outreach/iace_program/iace_certified_institutions.shtml

Neuman, J. H., & Baron, R. A. (1997). Aggression in the workplace. In R. Giacalone, & J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 37-67). London: Sage.

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, 391-419.

Newstrom, J. W., & Ruch, W. A. (1976). The ethics of business students: Preparation for a career. *AACSB Bulletin*, 21-29.

O'Leary-Kelly, A. M., Griffin, R. W., & Glew, D. J. (1996). Organization-motivated aggression: A research framework. *Academy of Management Review*, 21, 225–253.

Ponemon Institute LLC. (2012). The human factor in data protection. Retrieved May 31, 2012, from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf

Robertson, D. H., & Joselyn, R. W. (1974). Projective techniques in research. *Journal of Advertising Research*, 14, 27-31.

Robinson, S. L., & Bennett, R. J. (1997). Workplace deviance: Its definition, its nature, and its causes. In R. J. Lewicki, B. H. Sheppard, & R. J. Bies (Eds.), *Research on negotiation in organizations, Vol. 6* (pp. 3-28). Greenwich, CT: JAI Press.

Ruiz, J. M., Smith, T. W., & Rhodewalt, F. (2001). Distinguishing narcissism and hostility: Similarities and differences in interpersonal circumplex and five-factor correlates. *Journal of Personality Assessment*, 76(3), 537-555.

Ryff, C. D. (1989). Happiness is everything, or is it? Explorations on the meaning of psychological well-being. *Journal of Personality and Social Psychology*, 57(6), 1069-1081.

Ryff, C. D., & Keyes, C. L. M. (1995). The structure of psychological well-being revisited. *Journal of Personality and Social Psychology*, 69(4), 719-727.

Salmivalli, C. (2001). Feeling good about being bad to others? Remarks on self-esteem, hostility, and aggressive behavior. *Aggression and Violent Behavior*, 6, 375-393.

Sheppard, B. H., Lewicki, R. J., & Minton, J. W. (1992). *Organizational justice: The search for fairness in the workplace*. New York, NY: Lexington Books.

Short, J. F., Jr., & Nye, F. I. (1957-58). Reported behavior as a criterion of deviant behavior. *Social Problems*, 5(3), 207-213.

Shuptrine, F. K. (1979). Evaluating the ethics of marketing practices: Student perceptions. In N. Beckwith, M. M. Houston, S. Ward, R. Mittelstaedt, & K. B. Monroe (Eds.), *Educators Conferences Proceedings* (pp. 124-127). Chicago, IL: American Marketing Association.

Sieh, E. W. (1987). Garment workers: Perceptions of inequity and employee theft. *British Journal of Criminology*, 27, 174-191.

Skarlicki, D. P., & Folger, R. (1997). Retaliation in the workplace: The roles of distributive, procedural, and interactional justice. *Journal of Applied Psychology*, 82, 434-443.

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

Standage, T. (2002). The weakest link. *The Economist*, 365(8296), 11–16.

Stern, J. (2003). *Terror in the name of God: Why religious militants kill*. New York, NY: HarperCollinsPublishers Inc.

Steurer, S. J., Smith, L., & Tracy, A. (2001). *Three state recidivism study*. Washington, DC: Office of Correctional Education, U.S. Department of Education.

Storms, P. L., & Spector, P. E. (1987). Relationships of organizational frustration with reported behavioural reactions: The moderating effect of locus of control. *Journal of Occupational Psychology*, 60, 227–234.

Taylor, L., & Walton, P. (1971). Industrial sabotage: Motives and meanings. In S. Cohen (Ed.), *Images of Deviance* (pp. 219-245). Harmondsworth: Penguin Books Ltd.

Tucker, J. (1993). Everyday forms of employee resistance. *Sociological Forum*, 8, 25-45.

Twenge, J. M., & Campbell, W. K. (2003). Isn't it fun to get the respect that we're going to deserve?: Narcissism, social rejection, and aggression. *Personality & Social Psychology Bulletin*, 29(2), 261-272.

U.S. Department of Commerce, Economics and Statistics Administration, and the Executive Office of the President, Office of Management and Budget. (2011). Women in America: Indicators of social and economic well-being. Retrieved August 17, 2012, from http://www.whitehouse.gov/sites/default/files/rss_viewer/Women_in_America.pdf

Wallerstein, J. S., & Wyle, C. J. (1947). Our law-abiding lawbreakers. *Probation*, 25, 107-112.

Wolfer, L., & Roberts, J. C. (2008). A theoretical exploration of a drug court program based on client experiences. *Contemporary Drug Problems*, 35(2), 481-507.