2010

How Explanation Adequacy of Security Policy Changes Decreases Organizational Computer Abuse

Clay Posey
University of Arkansas at Little Rock, mcposey@ualr.edu

Tom L. Roberts
Louisiana Tech University, troberts@LaTech.edu

Paul Benjamin Lowry
Brigham Young University, paul.lowry.phd@gmail.com

Becky Bennett
Louisiana Tech University, rbennett@latech.edu

How Explanation Adequacy of Security Policy Changes Decreases Organizational Computer Abuse

Clay Posey
University of Arkansas at Little Rock
mcposey@ualr.edu

Tom L. Roberts
Louisiana Tech University
troberts@latech.edu

Paul Benjamin Lowry
Brigham Young University
Paul.Lowry.PhD@gmail.com

Becky Bennett
Louisiana Tech University
rbennett@latech.edu

ABSTRACT

We use Fairness Theory to help explain why sometimes security policy sometimes backfire and increase security violations. Explanation adequacy—a key component of Fairness Theory—is expected to increase employees' trust in their organization. This trust should decrease internal computer abuse incidents following the implementation of security changes.

The results of our analysis provide support for Fairness Theory as applied to our context of computer abuse. First, the simple act of giving employees advance notification for future information security changes positively influences employees' perceptions of organizational communication efforts. The adequacy of these explanations is also buoyed by SETA programs. Second, explanation adequacy and SETA programs work in unison to foster organizational trust. Finally, organizational trust significantly decreases internal computer abuse incidents. Our findings show how organizational communication can influence the overall effectiveness of information security changes among employees and how organizations can avoid becoming victim to their own efforts.

Keywords

Fairness theory, computer abuse, organizational trust, security training and awareness, explanation adequacy

INTRODUCTION

The need to secure sensitive organizational data is increasingly vital to organizations in today's global information environment. Although information security is a longstanding need, it has grown in importance over time with increased globalization and computing complexity. While most organizations had minimal security controls in place almost two decades ago, recent studies have shown that expenditures for security controls are rapidly rising. These increases are likely because security breaches and associated losses are also increasing at a rapid rate.

Although security agendas have traditionally focused on threats external to the organization, breaches stemming from internal employees are considered to be among the greatest threats to the security of organizational information systems. Although some research shows that individuals' perceptions of sanctions decrease misuse of internal systems by employees [1, 2], contrasting research points to an increased frequency of computer abuse soon after the imposition of changes to security policies and procedures [3]. These contrasting findings indicate there are likely scenarios where increased deterrence measures may backfire and create a paradox of increased—not decreased—internal computer abuse.

In this study, we explain how organizations can increase security yet avoid such a paradox by building on the underlying foundation of organization trust and Fairness Theory.

Fairness Theory

Fairness Theory [4, 5] explains the methods individuals use in order to provide explanations for various organizational events they perceive as unfair. A recent meta-analytic review showed that Fairness Theory can predict the results of various kinds of explanations. For our purposes, we apply Fairness Theory in the narrow context of negative organizational decisions where it has been very effective in allowing researchers to explain individuals' reactions to negative events and decisions [6-9]. From this perspective, Fairness Theory posits that when employees experience a negative organizational event they have an inherent need to assign blame or accountability to the decision maker—an individual, a group of individuals, or an organization—for the event.

Fairness Theory predicts that the type of explanation given and the e*xplanation's adequacy*—the extent to which explanations provided by the organization are clear, reasonable, and detailed [10]—are what will fundamentally determine whether an employee feels a decision is fair with regard to negative management decisions [6]. Explanation adequacy is an important concept in the study of organizational fairness as it also refers to informational fairness or information justice [11, 12]. Employees who feel a decision is fair are more likely

to accept and follow it, whereas employees who feel a decision is unfair are more likely to reject it. Fairness Theory predicts this process of reacting to a negative decision, and associated explanation (if any), as follows: When an employee experiences a negative event, this triggers "counterfactual reasoning in an effort to understand [the negative event]" [6, p. 671]. These *counterfactuals—Would*, *Could*, and *Should*—form the basis to which an employee compares the negative event as the individual places "what 'is' side by side with 'what might have been'" [4, pp. 5-6]. This contrastive perspective proffered by counterfactuals serves as a frame of reference for the individual [4]. The *Would counterfactual* is based on the hypothesized condition that would have resulted had a feasible, alternative decision been made. This counterfactual assists the individual in answering the question, "Would my well-being have been better off if this event had played out differently?" [10, p. 447]. The employee then evaluates the discrepancy between the actual and the hypothetical scenario with the magnitude of the difference having a direct bearing on perceived fairness. The larger the negative difference, the more likely a decision will be seen as unfair.

The other two counterfactuals largely determine whether the generated fairness/unfairness judgment becomes solidified. A *Could counterfactual* "addresses whether the negative event was under the decision maker's discretionary control" [6, p. 671]. To clarify, conduct that is discretionary describes another's choices among feasible alternatives [4]. Ceteris paribus, the more an employ considers a negative decision to be made under an employer's discretionary control, the more likely the employee will judge the decision as unfair. Similarly, *Could* counterfactuals answer the question of "Could the decision maker have acted differently: were there other feasible behaviors?" [10, p. 447]. If employees understand that different actions could not have been taken, they cannot realistically assign blame to the decision maker [4].

Should counterfactuals "address moral or ethical conduct and suggest that [individuals] also evaluate whether the decision maker acted in accordance with appropriate standards" [6, p. 671]. This assessment provides an individual with the answer as to whether the decision maker should have acted differently relative to a set of standards [4]. Anything perceived as unethical or immoral will generate a negative *Should* counterfactual, and will be much more likely to solidify an unfairness judgment. Strong *Should* counterfactuals can also emanate from the decision maker's deviation from standards based on industry norms, training, and so forth. A security example would be if an employee works with sensitive materials and is trained in the importance of using encryption to protect sensitive materials, they will generate a much more positive *Should* counterfactual if they are told that all organizational email communication must use a particular encryption standard than an employee without awareness of these standards or their purposes.

Advanced Notification of Security Changes

Advance notice is a vital component of fair systems. Brockner et al. [13] explained that procedures are unfair if decision makers implement them without regard for the legitimate concerns of those affected—such as reasonable preparation to deal with the adverse consequences of a decision. Accordingly, a security change will more likely be seen as unfair, and subsequently not be embraced, if an organizational simply rolls out a security change without explanation or with an explanation after-the-fact. The fundamental reason why this will occur—from a Fairness Theory perspective—is that the lack of timely explanation or a complete lack of explanation will increase the likelihood and strength of *Could* counterfactuals. Without prior notification and explanation, a decision is more likely to be seen as having no factual basis, heavy handed, or capricious. Conversely, a thoughtful and timely explanation can help an employee believe a new policy is reasonable and factual.

H1: Advance notification increases perceived explanation adequacy.

Organizational SETA Efforts and Explanation Adequacy

The construct of explanation adequacy\not only applies to whether advance notification is given but also to whether the explanation itself is sound and reasonable. Explanation adequacy can affect the generation of *Could* counterfactuals, because absent of explanation, one is not fully capable of determining whether other feasible options existed and hence whether the organization had control over the decision. In other words, these counterfactuals may not be realistic and thus result in an exaggerated magnitude. As a security example, suppose an employee does not understand that a three-character password is exponentially less secure than a ten-character password; such an employee is more likely to see a three-character password option as reasonable and that a new policy mandating ten-character passwords is not necessary and that the organization could have taken other approaches.

Given this background, it is not surprising that the organizational literature shows that "the failure to give an explanation—or the use of an inadequate one—can lead to negative employee reactions" [10, p. 453], especially in the event of unfavorable or constraining outcomes to employees. Conversely, when employees receive sincere, detailed explanations, they respond more positively to the associated change [10, 14, 15].

However, because security itself can be highly technical and arcane, logic and explanations may be inadequate—thus creating unrealistic or distorted counterfactuals—because employees may simply not understand the fundamental issues involved. Lack of understanding of security principles and standards may also cause misleading *Should* counterfactuals, as these are based on ethical, moral, and industry standards.

Organizations might be able to produce more positive counterfactuals in its employees if it has a formal SETA program. These programs can be especially effective because they "inform employees about their roles, and expectations surrounding their roles, in the observance of information security requirements" [16, p. 51]. Specifically, SETA programs are based on a comparative framework and are implemented (1) to improve employee awareness of *what* threats exist to organizational information assurance, (2) to train employees on *how* to perform their jobs in a secure manner, and, (3) to educate employees regarding *why* these threats exist. Accordingly, we define *organizational SETA efforts* as the degree with which an organization formally provides its employees with an awareness of what threats exist in the work environment, why these threats exist, and notification of how they can more securely engage in work activities. In addition, SETA programs represent a rather low-cost initiative relative to the increased costs of security breaches [17]. This educational process is vital in notifying employees of the behaviors that are not acceptable and provides the foundation on which organizations may reasonably improve their security posture if required.

H2: Appropriate SETA programs increase perceived explanation adequacy.

Organizational SETA Efforts and Organizational Trust

Changes to information security measures can negatively affect organizational members via changes to daily job tasks [18] and lead to increased job stress and insider abuse [3]. Such unfavorable conditions serve as the igniting spark for the counterfactual thinking process suggested by Fairness Theory [4]; however, organizations once again have the ability to decrease the discrepancy between "what is" and "what would, could, and should be" in the minds of employees by building organizational trust through SETA efforts. *Organizational trust* is defined as "one's expectations, assumptions, or beliefs about the likelihood that another's future actions will be beneficial, favorable, or at least not detrimental to one's interests" [19, p. 576] and is based on several key characteristics. Because many employees view additional information security measures as constraining and time consuming at the very least, organizational trust is developed largely from the organization's assurance to its employees that it will abide by and engage in actions of the least detrimental fashion by its adherence to those key characteristics.

When organizations properly design SETA efforts and engage their employees in them [20], these activities also provide the forum in which employees can better assess the organization's ability to properly handle information-security matters, one of the more significant aspects of organizational trust [21, 22]. Moreover, SETA programs provide organizations with the best opportunity to overtly express the standards by which they operate. In the end, these sets of guiding operational principles via SETA programs ultimately provide an instrument by which an employee is able to gauge the organization's actual security activities and whether the organization is worthy of the employees' continued trust.

H3: Appropriate SETA programs increase organizational trust.

Explanation Adequacy and Organizational Trust

Organizational trust is a key outcome of organizational fairness Because explanation adequacy equates to informational fairness or justice, organizational explanations can foster organizational trust and perceived support [23]. Employee trust will increase as management conducts activities with clear and open communication [23], but these explanations lose their efficacy and may even be counterproductive unless they are deemed sincere and believable [24]. This word-deed misalignment ultimately undermines trust in organizations. Providing both justifications and advance notice may therefore enhance perceived behavioral integrity and post-implementation trust [23]. In contrast, implementing new security policies without properly notifying employees might be considered a breach of trust that is viewed as suspicious, as having little credibility, and as manipulative [23]. Blau [25] argued that ''the establishment of exchange relationships requires others to reciprocate. Since social exchange requires others to reciprocate, the initial problem is to prove oneself trustworthy.'' Accordingly, actions that establish and reinforce trust therefore engender an obligation on the part of employees to reciprocate [23].

Organizational explanations for information-security activities that are deemed as adequate, thorough, reasonable, and timely by employees are likely to be perceived as candid communication. This openness is another key facet in employees' development of trust in their organizations. The building and maintaining of organizational trust is particularly important in the design and implementation of organizational security practices such as monitoring and surveillance, because these activities tend to produce feelings of distrust within organizational members. Stanton and Stam [18] note: "precipitous changes in the organization's monitoring and surveillance policies and practices are the ones most likely to raise eyebrows and erode the trust that employees have in their organization" (p. 75).

H4: Perceived explanation adequacy increases organizational trust.

Organizational Trust and Internal Computer Abuse

Trust is an important predictor of a number of key organizational outcomes including organizational citizenship behavior [26]. The outcome of the counterfactual process in our model—organizational trust—is an essential element in determining how

employees respond to negative organizational events. For example, the effects of employees' disagreements with managers [27], perceived psychological contract breaches [19], and organizational downsizing [28] are all attenuated by organizational trust. Organizations that enhance their information-security measures should also be able to leverage the positive influences of employees' trust to their benefit.

Employees who trust their organization are more likely to behave beneficially toward their organization because they believe the organization is looking out for them. Conversely, individuals who have little trust in their organization are more likely have been found to act in counterproductive [29] or antisocial ways [30]. Because organizational trust exists when employees believe that the actions of their organization "will be beneficial, favorable, or at least not detrimental to one's interests" [19, p. 576], employees who do not experience such beliefs are more likely to be self-serving [31] and deviant, because they expect the organization will not act in the best interest of the employee [30].

H5: Organizational trust decreases computer abuse.

METHODOLOGY

Data Collection

An online panel composed of 397 full-time employees from the banking, financial, and insurance industries was used to obtain data for testing our research model. To qualify for the study, each respondent had to utilize their organization's computer systems in fulfilling their daily job tasks. Anonymity was guaranteed for each respondent. Anonymity is important in obtaining honest, self-report responses to questions regarding a sensitive subject like internal computer abuse [32].

ANALYSIS AND RESULTS

We analyzed our theoretical model with the structural equation modeling program AMOS 16.0 and followed the two-step method suggested by prior methodological research. Factorial validity was established using standard approaches and common methods bias was not present. The final results are summarized in Figure 1.

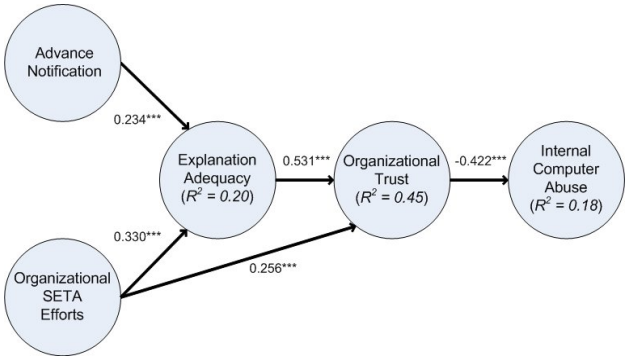

Figure 1. Model Testing Results

DISCUSSION

The results imply several practical implications. First, the results show how important organizational communication to insiders is. Individuals whose organizations make the effort to discuss information security changes prior to their implementation perceive a greater degree of explanation adequacy than those who were told after. This seemingly underestimated or overlooked action (i.e., a surprising 41% of our sample) by firms significantly relates to the variance exhibited in insiders' perception of explanation adequacy.

Second, organizational security education, training, and awareness programs built on the what, how, and why comparative framework suggested by security researchers [20] serves at least two main functions: (1) the programs provide the foundation from which organizational insiders can better gauge organizational communication efforts regarding information security initiatives; and, (2) the programs build the organizational trust beliefs of insiders as they show the competence and/or the benevolence of the organization. H inconsistencies in communication received and/or perceived by insiders could be detrimental to the effectiveness of the information security initiatives.

Third, adequate explanations also provide reasoning for information security initiatives thereby increasing trust within the organization. It is important to reiterate that these two variables—explanation adequacy and SETA efforts—explain nearly half of the variance in organizational trust perceptions in our results.

Finally and perhaps most importantly, this research shows that organizational trust derived from organizational communication efforts significantly decreases internal computer abuse within organizations. Individuals' trust in their organizations accounts for almost one-fifth of the self-reported abuses. More work is requisite to explore other variables that significantly relate to internal computer abuses; however, we feel that this research provides an important, initial step in assessing the antecedents of a construct of such interest to both information security researchers and practitioners.

REFERENCES

[1] J. D'Arcy, A. Hovav, D. Galletta, User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, 20 (2009) 79-98.
[2] D.W. Straub, Effective IS Security, Information Systems Research, 1 (1990) 255-276.
[3] A.P. Moore, D.M. Cappelli, R.F. Trzeciak, The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures, in, Software Engineering Institute: Carnegie Mellon University, 2008.
[4] R. Folger, R. Cropanzano, Fairness Theory: Justice as Accountability, in: J. Greenberg, R. Cropanzano (Eds.) Advances in Organizational Justice, Standford University

Press, Stanford, CA, 2001, pp. 1-55.
[5] R. Folger, R. Cropanzano, Organizational Justice and Human Resource Management, Sage Publications, Thousand Oaks, CA, 1998.
[6] S.W. Gilliland, M. Groth, R.C. Baker, A.E. Dew, L.M. Polly, J.C. Langdon, Improving applicant's reactions to rejection letters: An application of fairness theory, Personnel Psychology, 54 (2001) 669-703.
[7] J.R. McColl-Kennedy, B.A. Sparks, Application of Fairness Theory to Service Failures and Service Recovery, Journal of Service Research, 5 (2003) 251-266.
[8] C.D. Beugre, Reacting aggressively to injustice at work: a cognitive stage model, Journal of Business and Psychology, 20 (2005) 291-301.
[9] J.A. Colquitt, J.M. Chertkoff, Explaining Injustice: The Interactive Effect of Explanation and Outcome on Fairness Perceptions and Task Motivation, Journal of Management, 28 (2002) 591-610.
[10] J.C. Shaw, E. Wild, J.A. Colquitt, To justify or excuse?: A meta-analytic review of the effects of explanations, Journal of Applied Psychology, 88 (2003) 444-458.
[11] J.A. Colquitt, On the dimensionality of organizational justice: A construct validation of a measure, Journal of Applied Psychology, 86 (2001) 386-400.
[12] M.C. Kernan, P.J. Hanges, Survivor reactions to reorganization: Antecedents and consequences of procedural, within-group, and informational justice, Journal of Applied Psychology, 87 (2002) 916–928.
[13] J. Brockner, M. Konovsky, R. Cooper-Schneider, R. Folger, C. Martin, R.J. Bies, Interactive effects of procedural justice and outcome negativity on victims and survivors of job loss, Academy of Management Journal, 37 (1994) 397-409.
[14] J. Greenberg, Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts, Journal of Applied Psychology, 75 (1990) 561-568.
[15] D.M. Schweiger, A.S. DeNisi, Communication with employees following a merger: A longitudinal field experiment, Academy of Management Journal, (1991) 110-135.
[16] T.C. Fitzgerald, B.C. Coins, R.C. Herold, Information Security and Risk Management, in: H.F. Tipton, K. Henry (Eds.) Official (ISC) 2 Guide to the CISSP CBK, Auerbach, 2006, pp. 1-92.
[17] M.E. Whitman, Enemy at the gate: threats to information security, Communications of the ACM, 46 (2003) 91-95.
[18] J.M. Stanton, K.R. Stam, The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust, Information Today, Inc., Medford, NJ, 2006.
[19] S.L. Robinson, Trust and breach of the psychological contract, Administrative science quarterly, 41 (1996) 574-599.
[20] M.E. Whitman, H.J. Mattord, Principles of information security, Thomson Course Technology, 2009.
[21] J.J. Gabarro, The development of trust, influence, and expectations, in: J. Athos, J.J. Gabarro (Eds.) Interpersonal behaviors: Communication and understanding in relationships, Prentice Hall, Englewood Cliffs, NJ, 1978, pp. 290-303.
[22] R.C. Mayer, J.H. Davis, F.D. Schoorman, An integrative model of organizational trust, Academy of Management Review, (1995) 709-734.
[23] G.S. Alder, T.W. Noel, M.L. Ambrose, Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust, Information & Management, 43 (2006) 894-903.
[24] R.J. Bies, D.L. Shapiro, L.L. Cummings, Causal accounts and managing organizational conflict: Is it enough to say it's not my fault?, Communication Research, 15 (1988) 381-399.
[25] P.M. Blau, Exchange and power in social life, Wiley, New York, NY, 1964.
[26] L. Van Dyne, D. Vandewalle, T. Kostova, M.E. Latham, L.L. Cummings, Collectivism, propensity to trust and self-esteem as predictors of organizational citizenship in a non-work setting, Journal of Organizational behavior, 21 (2000) 3-23.
[27] M.A. Korsgaard, S.E. Brodt, E.M. Whitener, Trust in the face of conflict: The role of managerial trustworthy behavior and organizational context, Journal of Applied Psychology, 87 (2002) 312-319.
[28] A.K. Mishra, G.M. Spreitzer, Explaining how survivors respond to downsizing: The roles of trust, empowerment, justice, and work redesign, Academy of Management Review, (1998) 567-588.
[29] J.A. Colquitt, B.A. Scott, J.A. LePine, Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance, Journal of Applied Psychology, 92 (2007) 909-926.
[30] S. Thau, C. Crossley, R.J. Bennett, S. Sczesny, The relationship between trust, attachment, and antisocial work behaviors, Human Relations, 60 (2007) 1155-1179.
[31] H.H. Kelley, J. Thibault, Interpersonal relations: A theory of interdependence, Wiley, New York, NY, 1978.
[32] R.J. Bennett, S.L. Robinson, Development of a measure of workplace deviance, Journal of Applied Psychology, 85 (2000) 349-360.