

Organizational Citizenship Behavior regarding Information Security (OCB-S): Leadership Approach Perspective

Ofir Turel

Professor, Information Systems and Decision Sciences

Mihaylo College of Business and Economics

California State University, Fullerton

800 N. State College Blvd., SGMH-4160, Fullerton, CA, USA

Phone: +1 657 278-5613

Email: oturel@fullerton.edu

Zhengchuan Xu* (corresponding author)

Associate Professor, Information Management and Information Systems

Fudan University,

220 Handan Rd, Yangpu, Shanghai, China, Room 708, Siyuan Building

Phone: +86 21 250-11237

Email: zcxu@fudan.edu.cn

Ken Guo

Assistant Professor, Accounting

Mihaylo College of Business and Economics,

California State University, Fullerton

800 N. State College Blvd., SGMH-4395, Fullerton, CA, USA

Phone: +1 657 278-7029

Email: kguo@fullerton.edu

ORGANIZATIONAL CITIZENSHIP BEHAVIOR REGARDING SECURITY (OCB-S): LEADERSHIP APPROACH PERSPECTIVE

ABSTRACT

This study takes a relational perspective to introduce the concept of organizational citizenship behavior regarding security (OCB-S) and to examine its predictors. Utilizing social exchange and role theories, we develop a model explicating the indirect effects of the way information systems (IS) departments lead IS initiatives and manages its relationships with end-users on end-users' OCB-S. Based on survey data from 223 employees of Chinese firms, we demonstrate that IS departments' management approaches play an important role in influencing business users–information systems department exchange (BIX) and user perceptions regarding whether IS security is their responsibility (extra-role perceptions regarding security). These factors, in turn, influence the extent to which end-users engage in OCB-S. Theoretically, this study advances our understanding of end-user security-related behaviors and their antecedents. Practically, this study highlights the importance of business users–information systems department relationships and role perceptions for improving organizational security management.

Keywords: Organizational Citizenship Behavior regarding Security (OCB-S); Relational perspective; Leadership approach; Social exchange theory; Role theory

Introduction

Information security is an important issue in modern organizations because information systems (IS) will likely fail to deliver value gains if they are not secure and may even hurt the organization when information security fails. This paper aims to examine one particular

challenge in security management: end-user security-related behavior. End-users, i.e. employees who use IS for their work, have long been viewed as an insider threat to IS security. When using IS in ways which are inconsistent with recommended security management best-practices, such as failing to encrypt data or change passwords, end-users may inadvertently put important organizational data at risk and potentially threaten the effective use of information systems for supporting strategic and operational needs. In this study, we extend this perspective and suggest that end-users should not only be conceived as a potential problem; they can also be, if managed properly, a source for improving information security in organizations.

Given the importance of employee behaviors for organizational security management, a growing body of research has focused on understanding such behaviors, particularly in terms of policy compliance or violations. Factors that explain end-user information security policy violations or compliance include cost/benefit considerations (Bulgurcu, Cavusoglu, & Benbasat, 2010; Guo, Yuan, Archer, & Connelly, 2011; Hu, Xu, Dinev, & Ling, 2011), organizational sanctions (D'Arcy & Devaraj, 2012; D'Arcy, Hovav, & Galletta, 2009; Herath & Rao, 2009a; Kankanhalli, Teo, Tan, & Wei, 2003), workgroup/social norms (Bulgurcu et al., 2010; Guo et al., 2011; Herath & Rao, 2009b), perceived identity match (Guo et al., 2011), personal self-sanctions (Guo & Yuan, 2012), self-efficacy (Bulgurcu et al., 2010; Herath & Rao, 2009b; Johnston & Warkentin, 2010), moral reasoning/values (Hu et al., 2011; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009), neutralization (Siponen & Vance, 2010), learning through prior experience of security threats (Tu, Turel, Yuan, & Archer, 2015), perceived legitimacy (Son, 2011), habit (Vance, Siponen, & Pahnila, 2012), and organizational culture (Hu, Dinev, Hart, & Cooke, 2012).

Although this behavioral security literature has greatly advanced our understanding of the human factor in organizational information security management, there are two important issues that have been understudied. First, prior studies tend to have treated end-users as individuals making unilateral behavioral decisions. While it has merits by and in itself, such treatment may inadvertently oversimplify how end-users make behavioral decisions in typical work settings.

There are many groups of organizational members involved in information security (Guo, 2013a). In a typical organizational setting, the IS department is usually in charge of the overall management of information systems; It often works in collaboration with or as part of top management to implement and change IS in the organization. Even though the IS department may not be the sole leader of all IS projects, they are typically involved in initiating, managing and measuring the success of IS projects (Banker, Hu, Pavlou, & Luftman, 2011). The IS department is therefore perceived to be leading IS projects and it works closely with end-users on such projects, for instance through receiving inputs and providing suggested solutions, or sending demands, such as password or software package change, to employees (Gefen & Ridings, 2003). Consequently, end-users do not make behavioral decisions in an isolated manner; their relationships with the IS department and top management can have some influences on their security behaviors. For example, one might expect stronger attention to information security issues when the relationship with the IS department is excellent, as opposed to otherwise. Such intergroup relationships are not limited to security issues; they are rather prevalent in the general organizational environment and can promote positive behaviors such as knowledge sharing/collaboration (Trkman & Desouza, 2012) and effective human resources management (Sun, Aryee, & Law, 2007). Thus it is important, theoretically and practically, to examine the effects of intergroup relationships in the IS department - user context on information

security behaviors. Such relationships have been shown to be important for technology acceptance decisions (Gefen & Ridings, 2003), but not in for decisions regarding security behaviors.

Second, prior studies have largely focused on compliance and violation related to security policies, which represent in-role behaviors defined as behaviors associated with the defined job duties of employees. These studies mostly ignored the fact that users can go above-and-beyond their role, i.e., engage in extra-role behaviors such as organizational citizenship behaviors. Nevertheless, such extra-role behaviors can greatly benefit organizations (Organ, 1988; Organ, 1990; Organ, Podsakoff, & MacKenzie, 2006; Organ & Ryan, 1995). In other words, while the extant literature is “barking at the correct tree” (compliance, violation, etc.), there are other important “trees” it can and should focus on, namely Organizational Citizenship Behavior regarding Security (OCB-S), which encapsulates a narrow category of benevolent security behavior that has not been sufficiently studied in the literature (Guo, 2013b; Hsu, Shih, Hung, & Lowry, 2015; Posey, Roberts, Lowry, Bennett, & Courtney, 2013). OCB-S is a nuanced (IS security- focused) type of OCB. It is arguably important to focus on this nuanced OCB, because it seems to have stronger direct ties to IS security benefits, compared with broader types of extra-role behaviors, such as helping and caring for others. The latter group of behaviors can certainly be beneficial for the organization (Podsakoff, Whiting, Podsakoff, & Blume, 2009), but may have more indirect influence on security behaviors, which are the focus of this study. For instance, helping and being courteous to others may be less related to password changing practices compared with specifically encouraging people to change their passwords.

We aim to address the abovementioned gaps by taking a relational approach to examining predictors of OCB-S. Based on social exchange theory (Blau, 1964) and role theory (Biddle,

1979), we contend that end-user OCB-S is associated with how end-users perceive their relationship with IS departments (*Business User—IS Exchange*, or *BIX*) and the extent to which end-users see information security behaviors as extra- vs. inner-role (*Extra-Role Perception*). These two predictors reflect the social and economic exchange aspects of IS security management in organizations. IS departments rely on end-users to carry out security tasks when they use technology in their business activities, and this behavior can be driven by social reciprocity forces as well as the extent to which IS security behaviors are considered to be an integral part of one's job or as extra-role behaviors.

We further contend that the aforementioned predictors are associated with how IS departments manage work with end-users. We operationalize the “how” aspect as two general management approaches that IS departments can simultaneously adopt—namely *authoritarian* and *participative* approaches—to interacting with and leading end-users. We limit our investigation to the relationship between end-users and IS departments (in contrast to, for example, top management) because end-users and IS department are in the same hierarchical level in the organization and they often interact directly with each other on a daily basis. In IS projects, though, the IS department is often taking the lead or co-lead role (Banker et al., 2011). Hence, the interactions between the examined groups is relationship-based, with some leadership elements.

The study empirically tests the proposed model with Partial Least Squares (PLS) techniques applied to data collected from 223 employees in China. The results largely support the proposed model and show that the way IS departments manage their relationships with end-users influences their exchange relationship perceived by end-users as well as the perceptions of IS security tasks as extra-role behaviors. These factors, in turn, are a basis upon which employees

decide to engage in OCB-S, which is arguably an important, yet largely overlooked, IS security behavior.

Research Model and Hypotheses

Drawing on social exchange and role theories as well as the notions of authoritarian and participative approaches for management (see detailed theoretical discussion of these concepts in Appendix 1), and applying them to OCB-S, we propose a theoretical model depicted in Figure 1. The underlying logic is that the leadership approaches employed by the IS department influence how end-users perceive their relationship with the IS department as well as their roles in maintaining and promoting IS security. End-users will engage in OCB-S if they have good reciprocal exchange relationships with the IS department; and conversely, they will withhold their OCB-S efforts if they perceive IS security tasks as not part of their roles. These exchange and role perceptions, based on prior research (Clarke, 2013; Collins, Burrus, & Meyer, 2014; Lo, Ramayah, Min, & Songan, 2010; Markham, 2012), are argued to be influenced by the way the IS department interacts with users, i.e., its leadership approach, and the extent to which it adopts an authoritarian and participative leadership stance (A. Y. Zhang, Tsui, & Wang, 2011).

Effect of Business Users-IS Department Exchange on OCB-S

Applying social exchange theory, we argue that in an organization there exists a relationship between end-users and the IS department and that this relationship will influence how end-users engage with organizational information systems related tasks. We conceptualize this kind of relationship as *Business users-IS department exchange (BIX)*, which is based on the identity differences and boundaries between IS departments and their users (Gefen & Ridings, 2003). It is not uncommon that information systems are managed by a single unit in organizations- the IS department (Rathnam, Johnsen, & Wen, 2004). This centralized organizational structure,

however, creates an obvious point of friction between the IS department and end-users because IS departments manage information systems while end-users are responsible for their own business activities that the systems are intended to support (Applegate, McFarlan, & McKenney, 1996, p. 42). Such conflicts are inevitable in organizations due to differences between IS departments and users in terms of perceptions of reality (Gibson, Ivancevich, & Donnelly, 1988, pp. 304-313), goals, resources, culture (Cox, 2003), and role identities (Gefen & Ridings, 2003). Indeed, such tensions are fairly common (Applegate et al., 1996, p. 166; McKeen & Smith, 1996) and may contribute to end-user resistance to the implementation of information systems in organizations (c.f. Bhattacherjee & Hikmet, 2007; Lapointe & Rivard, 2005).

We contend that the quality of BIX will influence how end-users respond to information security tasks. In the case of low quality BIX, The IS department may not be perceived as a trustworthy partner, which is essential for OCB enactment (Mayer & Gavin, 2005; Robinson & Morrison, 1995). In such cases end-users may also develop stereotypes about IS people in terms of their business knowledge, skills and intentions (Gefen & Ridings, 2003) and security measures may be seen as barriers and obstacles that create troubles for users rather than as protective mechanisms (Adams & Blandford, 2005; Dourish, Grinter, de la Flor, & Joseph, 2004).

In contrast, in the case of high quality BIX, end-users may develop positive attitudes toward the IS department and have high levels of trust and confidence in IS people through attribution (Kelly, 1972). End-users in such cases will feel a stronger need to reciprocate in the exchange relationship with the IS department given what they feel is a friendly and committed service given to them by friends (Eisenberger, Armeli, Rexwinkel, Lynch, & Rhoades, 2001; L. M. Shore, Bommer, Rao, & Seo, 2009), and consequently will likely be more accommodating to security measures and more willing to help IS departments even if it requires extra efforts from

them. Similar relationships between exchange relationship quality and organizational citizenship behaviors, as a form of reciprocity, have been demonstrated in many management studies (Deluga, 1994; Graen & Uhl-Bien, 1995; Hui, Law, & Chen, 1999; Lapierre & Hackett, 2007; van Dyne, Kamdar, & Joireman, 2008; Wat & Shaffer, 2005) as well as in studies focusing on IS user interactions with team members (Yu & Chu, 2007). Extending this view to Business users-IS department relationships, the following hypothesis is proposed:

H1: *The quality of Business users -IS department exchange is positively related to end-user OCB-S.*

Effect of Perceiving IS Security Behavior as Extra-Role on OCB regarding Information Security

IS security is often not seen as an end-users' task (Besnard & Arief, 2004). Rather, it is typically viewed as the responsibility of IS departments (Albrechtsen & Hovden, 2009). In other words, end-users may argue that dealing with IS security issues is not part of their roles in general business activities such as sales, accounting, operations management, etc. From the social exchange theory perspective, they focus on economic exchange that involves economic calculations of whether their compensation or punishment (i.e. what they get) is in any way based on security tasks they perform (i.e. part of what they have to give); and typically it is not.

As a result of this economic-exchange calculus, users may not care about security as much as they care about their main business tasks (e.g., generating sales) (Song, Tsui, & Law, 2009). When this happens, security is perceived as an extra role behavior and users are likely to be less prone to engage in organizational citizenship behaviors related to security maintenance (Morrison, 1994). Given typical economic-exchange considerations, users will focus more on in-role tasks rather than on what they perceive to be as extra-role tasks (Bakker, Demerouti, &

Verbeke, 2004; MacKenzie, Podsakoff, & Ahearne, 1998; Van Dyne & LePine, 1998). This argument is consistent with findings regarding the effects of job performance expectations on security behaviors (Guo et al., 2011). Conversely, if end-users perceive security tasks as in-role, they will likely put forth more efforts toward those tasks, and even go above-and-beyond to sustain security; i.e., present higher levels of OCB-S (Morrison, 1994). Therefore, it is hypothesized that:

H2: *End-user extra-role perceptions about IS security behaviors are negatively related to end-user OCB-S*

Effects of Leadership Approaches Exercised by the IS department on BIX and Extra-role Perceptions

An authoritarian approach, as described in the Theoretical Background section, can result in various outcomes relevant for this study. First, it can create animosity (Falbe & Yukl, 1992) and increased perceived distance (Gefen & Ridings, 2003) between the IS department and the end-users. This happens because forcing people to act according to someone else's view takes away behavioral freedom which is often cherished by individuals (S. S. Brehm & Brehm, 1981; Woller, Buboltz, & Loveland, 2007), and this results in negative emotions and resistance targeted toward externally enforced policies (J. W. Brehm, 1966). In such cases, social exchange between the IS department and end-users is infringed, and the relationship becomes focused on economic exchange, according to which users perform the required actions as a means to avoid punishment (e.g., compliance) and not out of dedication or reciprocation (L. M. Shore et al., 2009; L.M. Shore, Tetrick, Lynch, & Barksdale, 2006; Song et al., 2009). At one extreme, the relationship could become hostile and cause a complete failure of IS implementation projects (Lapointe & Rivard, 2005). It is not surprising that punishment, a common tool of the

authoritarian approach, has been found ineffective in preventing end-user security violations (Guo et al., 2011; Siponen & Vance, 2010). Hence, when an authoritarian approach is taken by the IS department, the relationship becomes unidirectional, there is no desire to reciprocate, and consequently the quality of the social exchange between the department and end-users is expected to diminish. Hence:

H3: *Authoritarian approach of IS leadership is negatively related to Business User-IS department exchange.*

In addition, when authoritarian approach is taken by the IS department, end-users will be less likely to take ownership of those policies and procedures that are pushed down onto them, and may be suspicious toward them, not knowing whether they serve their best interest or not (Lapointe & Rivard, 2005; van Offenbeek, Boonstra, & Seo, 2013). As a result, users will be more likely to treat security tasks as belonging to the IS department and as being above and beyond their roles, i.e., extra-role. They, in such cases, will likely resist theses "duties" and will not want to do them (Bakker et al., 2004; MacKenzie et al., 1998; Van Dyne & LePine, 1998). In such situations users are likely to perceive these behaviors as the responsibility of whomever took their control and made decisions for them, without consulting with them (S. S. Brehm & Brehm, 1981; Dillard & Shen, 2005; Johnson & Buboltz, 2000), that is, the IS department.

Hence:

H4: *Authoritarian approach of IS leadership is positively related to end-user extra-role perceptions regarding IS security behaviors.*

Similar to the authoritarian approach discussed above, participative approach, as described in the Theoretical Background section, can result in outcomes relevant for this study, albeit in the

opposite direction to those stemming from authoritarian approach. The participative approach emphasizes collaboration between the IS department and users; it encourages ongoing communications and collaboration for the development of IS and security policies. Prior research has suggested that end-user participation can improve the effectiveness of security management (Adams & Blandford, 2005; Albrechtsen & Hovden, 2009; Spears & Barki, 2010). A participative approach can improve bidirectional communications between end-users and the IS department, better engage end-users in the security management processes, and better align security procedures with end-user needs and practices. As a result, end-users may feel that they need to reciprocate the positive and caring treatment they receive from the IS department (Coyle-Shapiro, 2002; Wasko & Faraj, 2000). This notion of reciprocity by employees who are given a chance to have their say in determining procedures and choices have been demonstrated across functional business domains (Allen, Shore, & Griffeth, 2003; Aryee & Chay, 2001; Aryee, Chen, & Budhwar, 2004; Fang, Palmatier, & Evans, 2008; Gruen, Summers, & Acito, 2000). Accordingly, we hypothesize that a participative approach enacted by the IS department will promote social reciprocity, and ultimately improve the business users-IS department social exchange:

H5: *Participative approach of IS leadership is positively related to Business Users-IS department social exchange.*

Similarly, given that in participatory environments users develop ownership of the developed product (security policies and role expectations in our case) (Adams & Blandford, 2005; Albrechtsen & Hovden, 2009; Spears & Barki, 2010), and see the participatory tasks as more related to their in-role (Brandes, Dharwadkar, & Wheatley, 2004; Groth, 2005; Lin, Hung, & Chiu, 2008), they will likely be more acceptant of security tasks as in-role rather than as extra-

role. In essence, their involvement with and influence on IS issues, including IS security policies, will make them feel that IS security management is at least a small part of their job and less as extra-role. Hence:

H6: *Participative approach of IS leadership is negatively related to end-user extra-role perceptions regarding IS security behaviors.*

Research Method and Results

Measures and Data Collection

Measures were based on adaptations from valid and reliable scales. Given that the study was done in Chinese firms, we employed forward-backward translation procedure. The final English version of scales and their sources are given in Appendix 2. The survey was completed by 223 end-users (average age=33) in select companies located in China. Further details about data collection and the sample are given in Appendix 3.

Results

SmartPLS 2.0 (Ringle, Wende, & Will, 2005) was used for validating the proposed research model. A number of factors were included as control variables: age, gender, job position, and education, in order to account for their possible effects on survey responses. An examination of common method bias alleviated such concerns regarding the data (see Appendix 4, section A4.1). The measurement model was valid (See Appendix 4, section A4.2). Hence, we proceeded with model estimation.

The hypotheses were assessed with bootstrapping with 500 re-samples in SmartPLS 2.0. The results are depicted in Figure 2. As the figure shows, the model explained 49% of the variance in *business users-IS department exchange (BIX)*, 17% in *extra-role perceptions regarding security*

(*ER*), and 18% in *organizational citizenship behavior regarding security (OCB-S)*. Consistent with the research model, *BIX* ($\beta = 0.23$, $p < 0.05$) and *ER* ($\beta = -0.28$, $p < 0.01$) had significant positive and negative effects, respectively, on *OCB-S*, thereby supporting H1 and H2. Additionally, *authoritarian approach (AA)* ($\beta = -0.38$, $p < 0.001$) and *participative approach (PA)* ($\beta = 0.44$, $p < 0.001$) had significant negative and positive effects, respectively, on *BIX*, lending support for H3 and H5. *Authoritarian approach* had a significant positive effect on *extra-role perceptions* ($\beta = 0.36$, $p < 0.01$), thereby demonstrating support for H4. However, *participative approach* seemed to be a less salient factor, at least in the examined context, and did not have a significant effect on *extra-role perceptions*. Thus, H6 was not supported. The influences of all control variables, including age, gender, job level, and education, were not significant. Post hoc analyses (e.g., effect sizes) are described in Appendix 5.

Discussion

What are key relational drivers of OCB-S in organizations? This study shows that similar to other organizational citizenship behaviors, OCB-S is driven by social exchange relationships. Nevertheless it points to a special type of relationship—between the IS department and end-users—which matters for OCB-S and indirectly, perhaps, to IS security management in organizations. The study further shows that OCB-S is diminished by perceiving IS security to be “someone else’s responsibility”, i.e., as an extra-role task. The business-IS relational exchange and extra-role perceptions were in turn influenced by the leadership approaches the IS department has adopted in order to work with business users, and specifically the extent to which the IS department engaged in authoritarian and participative approaches. Hence, this study is useful in (1) showing that OCB-S can exist and may be relevant for future security behavior

research, and (2) pointing to its relational predictors based on social exchange (Blau, 1964) and role (Biddle, 1979) theories.

Theoretical Implications

The results of this study have important theoretical implications for the IS security management literature. First of all, this study extends the range of positive IS security behaviors organizations should possibly encourage, to include OCB-S. The existing IS security management literature has largely focused on negative behaviors such as policy violations and malicious behaviors. Positive behaviors such as OCB-S have not drawn much attention, even though they should (Guo, 2013b; Posey et al., 2013). Our study shows that OCB-S is quite prevalent (mean of 4.94) and that employees differ in their engagement in OCB-S (std. dev. of 1.58). Hence, future research is encouraged to further explore this type of behavior, its predictors and outcomes by relying on the vast management literature on OCB; and this study can serve as a platform for such endeavors.

Furthermore, taking a relational approach, this study contributes to the literature by explicitly taking into consideration the social relationship between IS departments and users. The existing IS security management literature has largely focused on individual-level factors such as cost-benefits calculus while paid less attention to the impact IS departments can have on IS security behaviors (see reviews in D'Arcy & Herath, 2011; Guo, 2013b; Siponen & Vance, 2014). In this study we examined the effect of the relationship between end-user and IS management (business user-IS exchange; or BIX) by drawing on social exchange theory (Blau, 1964). Future research can extend the relational and social-exchange view taken in this study to further examine how relationships between many entities such as top management, the IS department and users influence security-related behaviors.

A third major contribution of this study is in pointing to the need to focus on what end-users perceive to be in-role vs. extra-role responsibilities. While this psychological distinction has shown to have important implications for employee behaviors (Morrison, 1994), it has been largely overlooked in IS research. This may be an important omission in the context of IS security because security matters are often seen as not “belonging” to end-users and are not perceived to be an integral part of their jobs (Besnard & Arief, 2004). The results show that psychologically classifying IS security tasks as in- vs. extra-role does matter in terms of how users decide to engage in positive security behaviors such as OCB-S. They further show that employees believe, at least to some extent but not fully, that IS security is part of their job (mean of 3.0) and that they differ in their perceptions of IS security responsibilities (std. dev. of 1.73, lower quartile score of 1.25 and upper quartile score of 4). This implies that quite a few organizational end-users see their job roles rather disjoint from information security responsibilities. Future research may further explore the predictors and consequences of the role responsibility division IS users might have in their minds.

Fourth, this study contributes to the IS security management literature by examining the effects of the IS departments’ leadership approaches and the way it collaborates with and communicates policies to IS users. While prior studies focus on the existence and nature of policies (see reviews in D’Arcy & Herath, 2011; Guo, 2013b; Siponen & Vance, 2014) and how end-users make unilateral behavioral decisions, they rarely discuss how the IS department’s leadership approaches may matter too, and influences IS users’ security behaviors. By drawing on social exchange (Blau, 1964) and role (Biddle, 1979) theories, we examined the effects of two general approaches that IS departments use for working with business users: authoritarian approach and participative approach. The results suggest that an authoritarian-oriented approach will likely

dampen the work relationships between end-users and IS people and cause end-users to treat security tasks as extra-role behaviors. IS management with a participative approach, on the other hand, will likely improve the relationships between end-users and the IS department. Hence, future research can further examine how the way the IS department interacts and works with IS users can affect their perceptions and ultimately their desirable and undesirable IS security behaviors.

Lastly, this study extends the range of organizational citizenship behaviors management research has focused on. The management literature has focused on helping, courtesy, and civil behaviors that are targeted toward other individuals and the organization in non-IS contexts (Lapierre & Hackett, 2007; Lee, Wu, & Hong, 2007; LePine, Erez, & Johnson, 2002; Organ et al., 2006). This study demonstrates the OCB can be related to IS issues, and specifically to IS security management. Hence, both management and IS research are encouraged to further examine this newly conceptualized citizenship behavior.

Managerial Implications

The results of this study offer several implications for organizational IS security management. First, echoing prior research (Adams & Sasse, 1999), this study highlights the importance of treating end-users as partners rather than as enemies to security management. Although they may cause inadvertent security risks, end-users will appreciate the importance of security and perhaps more importantly be willing to engage in OCB-S.

Second, the work relationship between end-users and IS departments plays an important role in driving security behaviors. When users have a good relationship with the IS department, they will be more willing to do something in return to help IS department by engaging in OCB-S.

There are many things IS departments can do in this regard. For example, they may consider end-users' input and the impacts on their job when designing and implementing security measures, in order to engage end-users and promote the relationship with them. Moreover, the IS department can be invited to business unit events, and vice versa. In addition, this relationship could be a metric tracked by management.

Our results indicate that taking a participative management approach can help in this regard, and that taking an authoritarian approach can be harmful. The positive impact of participative approach ($\beta=0.44$) overshadows the negative impact of an authoritative approach ($\beta=-0.38$) on perceived relationship quality, and this difference was significant ($p<0.001$). Hence, IS departments should try to adopt, to the extent possible, a participative approach and avoid, to the extent possible, an authoritative approach. Looking at the difference between the participative and authoritative scores, the merits of this approach become apparent. This score had significant positive correlation with BIX and OCB-S (0.69 and 0.38, $p<0.001$) and negative correlation with extra-role perceptions (-0.39, $p<0.001$). To do so, organizations can encourage communication and collaboration between IS people and users, or use social events for promoting informal friendships. They can also decrease its authoritative approach by using the same means stated above and demonstrating to users how they were involved in formulating policies. The efficacy of such interventions and their boundary conditions, though, should be examined in future research.

Third, end-users' perceptions about their roles in IS security management influence their willingness to engage in OCB-S. Thus IS departments should encourage end-users to take responsibilities regarding IS security, for instance, through ongoing training and workshops emphasizing IS security and its importance for people's jobs can help in this regards.

Limitations Pointing to Future Research

Several limitations should be considered. First, the cultural context of this study was unique, we did not account for between-industry differences, and the study relied on cross-sectional data. The generalizability of the results to non-Chinese settings and the potential impacts of industry on the examined processes may require further research, ideally with longitudinal designs to overcome the cross-sectional limitation of the data. Second, we collected data by using self-report questionnaires. Although the instruments used were valid and reliable, future research may collect data from different sources and or use longitudinal designs for improving causality arguments. Third, we measured the relational factors such as BIX and IS management approaches as perceived by end-users. Even though these perceptions rather than the actual relationship drive action, future research may examine how IS departments evaluate their relationships with end-users and what specific management approach they take. Such research would be able to corroborate and extend the findings of the current study. In addition, it would be desirable to consider a broader set of relationships and leadership influences, not just between the IS department and users, but also between users and their supervisors, the top management team, etc., OCB-S has been conceptualized as targeting both the organization and individuals. Consistent with the OCB literature, while both types stem from relational and role perceptions (L. J. Williams & Anderson, 1991), future research may examine nuanced predictors and outcomes of OCB-S-individual and OCB-S-organization. Moreover, our perspective assumes that the IS department assumes, at least in part, some leadership role in IS projects, including IS security matters. This, however, may not always be the case and exceptions to this assumption should be examined in future research.

Fourth, we observed no association between participation and extra role perceptions. Future research may provide a more nuanced analysis of this association; it is possible that at extreme levels of participation, participation becomes a distraction for one's main job duties (e.g., too many non-job related committees), and that in such cases extra-role perceptions may be augmented. This possible non-linear effect was tested post-hoc and was not observed in this study (no function fitted to the data produced a positive association at high levels of participation). However, it may be possible if extreme levels of participation exist. Such cases can be found in future research, and this may allow testing the proposed complex association.

Fifth, we examined a nuanced type of OCB here given the assumption that it likely better predicts security behaviors compared to general OCB. This assumption and the associations between general OCB and OCB-S may be examined in future research. Lastly, it will be interesting to extend our model and find contextual boundary conditions for the effect of leadership approaches on role and relationship perceptions as well as their translation into OCB-S.

Conclusion

This study sought to expand the literature on positive IS security behaviors by introducing a relationship- and role-based lens of analysis and focusing on arguably important, yet understudied IS security behavior, namely organizational citizenship behavior regarding IS security. Relying on social exchange and role theories we developed a model explaining OCB-S. The results show that OCB-S is driven by role and relational perceptions of IS users, which are in turn influenced by the way IS departments work with or lead their users regarding IS matters. Hence, we point to the need to further examine OCB-S, its predictors and consequences, and to

further focus on the way security policies and requirements are implemented, rather than merely on their existence and nature.

References

- Adams, A., & Blandford, A. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies*, 63(1-2), 175-202.
- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 41-46.
- Adler, P. S., & Borys, B. (1996). Two types of bureaucracy: Enabling and coercive. *Administrative Science Quarterly*, 41(1), 61-89.
- Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, 28(6), 476-490.
- Allen, D. G., Shore, L. M., & Griffeth, R. W. (2003). The role of perceived organizational support and supportive human resource practices in the turnover process. *Journal of Management*, 29(1), 99-118. doi:10.1177/014920630302900107
- Applegate, L. M., McFarlan, F. W., & McKenney, J. L. (1996). *Corporate Information Systems Management: The Issues Facing Senior Executives*. Chicago: Irwin.
- Aryee, S., Budhwar, P. S., & Chen, Z. X. (2002). Trust as a mediator of the relationship between organizational justice and work outcomes: test of a social exchange model. *Journal of Organizational Behavior*, 23(3), 267-285. doi:10.1002/job.138
- Aryee, S., & Chay, Y. W. (2001). Workplace justice, citizenship behavior, and turnover intentions in a union context: Examining the mediating role of perceived union support and union instrumentality. *Journal of Applied Psychology*, 86(1), 154-160. doi:10.1037//0021-9010.86.1.154
- Aryee, S., Chen, Z. X., & Budhwar, P. S. (2004). Exchange fairness and employee performance: An examination of the relationship between organizational politics and procedural justice. *Organizational Behavior and Human Decision Processes*, 94(1), 1-14. doi:10.1016/j.obhdp.2004.03.002
- Aycan, Z., Schyns, B., Sun, J. M., Felfe, J., & Saher, N. (2013). Convergence and divergence of paternalistic leadership: A cross-cultural investigation of prototypes. *Journal of International Business Studies*, 44(9), 962-969. doi:10.1057/jibs.2013.48
- Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *Mis Quarterly*, 35(4), 831-858.
- Bakker, A. B., Demerouti, E., & Verbeke, W. (2004). Using the job demands-resources model to predict burnout and performance. *Human Resource Management*, 43(1), 83-104. doi:10.1002/hrm.20004
- Banker, R. D., Hu, N., Pavlou, P. A., & Luftman, J. (2011). CIO reporting structure, strategic positioning, and firm performance. *Mis Quarterly*, 35(2), 487-504.
- Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, 23(3), 253-264.
- Bhattacherjee, A., & Hikmet, N. (2007). Physicians' resistance toward healthcare information technology: A theoretical model and empirical test. *European Journal of Information Systems*, 16, 725-737.
- Biddle, B. J. (1979). *Role Theory: Expectations, Identities, and Behaviors*. New York: Academic Press.
- Blau, P. M. (1964). *Exchange and Power in Social Life*. New York, NY: Wiley.

- Brandes, P., Dharwadkar, R., & Wheatley, K. (2004). Social exchanges within organizations and work outcomes - The importance of local and global relationships. *Group & Organization Management*, 29(3), 276-301. doi:10.1177/1059601103257405
- Brehm, J. W. (1966). *A theory of psychological reactance*. New York, NY: Academic Press.
- Brehm, S. S., & Brehm, J. W. (1981). *Psychological reactance: a theory of freedom and control*. New York, NY: Academic Press.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study on rationality-based beliefs and information security awareness. *Mis Quarterly*, 34(3), 523-548.
- Chakravarthy, B., & Gargiulo, M. (1998). Maintaining leadership legitimacy in the transition to new organizational forms. *Journal of Management Studies*, 35(4), 437-456. doi:10.1111/1467-6486.00104
- Chen, Y., Ramamurthy, K., & Wei, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157-188.
- Choi, J. N. (2007). Change-oriented organizational citizenship behavior: effects of work environment characteristics and intervening psychological processes. *Journal of Organizational Behavior*, 28(4), 467-484. doi:10.1002/job.433
- Clarke, S. (2013). Safety leadership: A meta-analytic review of transformational and transactional leadership styles as antecedents of safety behaviours. *Journal of Occupational and Organizational Psychology*, 86(1), 22-49. doi:10.1111/j.2044-8325.2012.02064.x
- Cohen, J. (1992). A power primer. *Psychological Bulletin*, 112(1), 155-159.
- Collins, B. J., Burrus, C. J., & Meyer, R. D. (2014). Gender differences in the impact of leadership styles on subordinate embeddedness and job satisfaction. *Leadership Quarterly*, 25(4), 660-671. doi:10.1016/j.lequa.2014.02.003
- Cox, T., Jr. (2003). Cultural diversity in organizations: Intergroup conflict. In J. S. Ott, S. J. Parkes, & R. B. Simpson (Eds.), *Classic Readings in Organizational Behavior* (3rd ed., pp. 263-273): Thomson Learning.
- Coyle-Shapiro, J. A. M. (2002). A psychological contract perspective on organizational citizenship behavior. *Journal of Organizational Behavior*, 23(8), 927-946. doi:10.1002/job.173
- D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, 43(6), 1091-1124.
- D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643-658.
- D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), 79-98. doi:10.1287/isre.1070.0160
- Deluga, R. J. (1994). SUPERVISOR TRUST BUILDING, LEADER MEMBER EXCHANGE AND ORGANIZATIONAL CITIZENSHIP BEHAVIOR. *Journal of Occupational and Organizational Psychology*, 67, 315-326.
- Den Hartog, D. N., De Hoogh, A. H. B., & Keegan, A. E. (2007). The interactive effects of belongingness and charisma on helping and compliance. *Journal of Applied Psychology*, 92(4), 1131-1139. doi:10.1037/0021-9010.92.4.113
- Dierdorff, E. C., Rubin, R. S., & Bachrach, D. G. (2012). Role expectations as antecedents of citizenship and the moderating effects of work context. *Journal of Management*, 38(2), 573-598.
- Dillard, J. P., & Shen, L. J. (2005). On the nature of reactance and its role in persuasive health communication. *Communication Monographs*, 72(2), 144-168. doi:10.1080/03637750500111815

- Dourish, P., Grinter, R. E., de la Flor, R. D., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 391-401.
- Dulebohn, J. H., Bommer, W. H., Liden, R. C., Brouer, R. L., & Ferris, G. R. (2012). A meta-analysis of antecedents and consequences of leader-member exchange: Integrating the past with an eye toward the future. *Journal of Management*, 38(6), 1715-1759.
- Eisenberger, R., Armeli, S., Rexwinkel, B., Lynch, P. D., & Rhoades, L. (2001). Reciprocation of perceived organizational support. *Journal of Applied Psychology*, 86(1), 42-51. doi:10.1037//0021-9010.86.1.42
- Falbe, C. M., & Yukl, G. (1992). Consequences for managers of using single influence tactics and combination of tactics. *Academy of Management Journal*, 35(3), 638-652. doi:10.2307/256490
- Fang, E., Palmatier, R. W., & Evans, K. R. (2008). Influence of customer participation on creating and sharing of new product value. *Journal of the Academy of Marketing Science*, 36(3), 322-336. doi:10.1007/s11747-007-0082-9
- Farh, J., Cannella, A. A., & Lee, C. (2006). Approaches to scale development in Chinese management research. *Management and Organization Review*, 2(3), 301-318.
- Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), 39-50.
- Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security - A survey and classification of the research area. *Computers & Security*, 30(8), 748-769. doi:10.1016/j.cose.2011.08.002
- Gefen, D., & Ridings, C. (2003). IT Acceptance: Managing User - IT Group Boundaries. *The Data Base for Advances in Information Systems*, 34(3), 25-40.
- Gibson, J. L., Ivancevich, J. M., & Donnelly, J. H., Jr. (1988). *Organizations: Behaviors, Structure, Processes* (6th ed.). Plano, Texas: Business Publications, Inc.
- Goleman, D. (2000). Leadership that gets results. *Harvard Business Review*, 78(2), 78-+.
- Graen, G. B., & Uhl-Bien, M. (1995). Relationship-based approach to leadership: Development of leader-member exchange (LMX) theory of leadership over 25 years: Applying a multi-level multi-domain perspective. *Leadership Quarterly*, 6(2), 219-247.
- Groen, B. A. C., Wouters, M. J. F., & Wilderom, C. P. M. (2012). Why do employees take more initiatives to improve their performance after co-developing performance measures? A field study. *Management Accounting Research*, 23(2), 120-141.
- Groth, M. (2005). Customers as good soldiers: Examining citizenship behaviors in Internet service deliveries. *Journal of Management*, 31(1), 7-27. doi:10.1177/0149206304271375
- Gruen, T. W., Summers, J. O., & Acito, F. (2000). Relationship marketing activities, commitment, and membership behaviors in professional associations. *Journal of Marketing*, 64(3), 34-49. doi:10.1509/jmkg.64.3.34.18030
- Guo, K. H. (2013a). Revisiting the human factor in organizational information security management. *ISACA Journal*, 6, 37-41.
- Guo, K. H. (2013b). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, 32, 242-251.
- Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, 49(6), 320-326.
- Guo, K. H., Yuan, Y., Archer, N. P., & Connolly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203-236.
- Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks, CA: SAGE Publications.

- Hambley, L. A., O'Neill, T. A., & Kline, T. J. B. (2007). Virtual team leadership: The effects of leadership style and communication medium on team interaction styles and outcomes. *Organizational Behavior and Human Decision Processes*, 103(1), 1-20. doi:10.1016/j.obhdp.2006.09.004
- Haun, S., Steinmetz, H., & Dormann, C. (2011). Objective work–nonwork conflict: From incompatible demands to decreased work role performance. *Journal of Vocational Behavior*, 79(2), 578-587.
- Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts of information security management. *Journal of Strategic Information Systems*, 20(4), 373-384.
- Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.
- Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-125.
- Hofmann, D. A., & Morgeson, F. P. (1999). Safety-related behavior as a social exchange: The role of perceived organizational support and leader-member exchange. *Journal of Applied Psychology*, 84(2), 286-296. doi:10.1037/0021-9010.84.2.286
- Hofmann, D. A., Morgeson, F. P., & Gerras, S. J. (2003). Climate as a moderator of the relationship between leader-member exchange and content specific citizenship: Safety climate as an exemplar. *Journal of Applied Psychology*, 88(1), 170-178. doi:10.1037/0021-9010.88.1.170
- Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security effectiveness. *Information Systems Research*, 26(2), 282-300.
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-659.
- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6), 54-60.
- Hui, C., Law, K. S., & Chen, Z. X. (1999). A structural equation model of the effects of negative affectivity, leader-member exchange, and perceived job mobility on in-role and extra-role performance: A Chinese case. *Organizational Behavior and Human Decision Processes*, 77(1), 3-21. doi:10.1006/obhd.1998.2812
- Ifinedo, P. (2015). *Effects of Organizational Citizenship Behavior and Social Cognitive Factors on Employees' NonMalicious Counterproductive Computer Security Behaviors: An Empirical Analysis*. Paper presented at the International Conference on Information Resource Management.
- Johnson, P., & Buboltz, W. C. (2000). Differentiation of self and psychological reactance. *Contemporary Family Therapy*, 22(1), 91-102.
- Johnston, A. C., & Warkentin, M. E. (2010). Fear appeals and information security behaviors: An empirical study. *Mis Quarterly*, 34(3), 549-566.
- Kahai, S. S., Sosik, J. J., & Avolio, B. J. (1997). Effects of leadership style and problem structure on work group process and outcomes in an electronic meeting system environment. *Personnel Psychology*, 50(1), 121-146. doi:10.1111/j.1744-6570.1997.tb00903.x
- Kamdar, D., & van Dyne, L. (2007). The joint effects of personality and workplace social exchange relationships in predicting task performance and citizenship performance. *Journal of Applied Psychology*, 92(5), 1286-1298.
- Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23, 139-154.
- Kelly, H. H. (1972). Attribution in social interaction. In E. E. Jones, D. E. Kanouse, H. H. Kelly, R. E. Nisbett, S. Valins, & B. Weiner (Eds.), *Attribution: Perceiving the causes of behavior* (pp. 1-27). Morristown, N.J.: General Learning Press.

- Lapierre, L. M., & Hackett, R. D. (2007). Trait conscientiousness, leader-member exchange, job satisfaction and organizational citizenship behaviour: A test of an integrative model. *Journal of Occupational and Organizational Psychology*, 80, 539-554. doi:10.1348/096317906x154892
- Lapointe, L., & Rivard, S. (2005). A multilevel model of resistance to information technology implementation. *Mis Quarterly*, 29(3), 461-491.
- Lee, T. Z., Wu, C. H., & Hong, C. W. (2007). An empirical investigation of the influence of safety climate on organizational citizenship behavior in Taiwan's facilities. *International Journal of Occupational Safety and Ergonomics*, 13(3), 255-269.
- LePine, J. A., Erez, A., & Johnson, D. E. (2002). The nature and dimensionality of organizational citizenship behavior: A critical review and meta-analysis. *Journal of Applied Psychology*, 87(1), 52-65. doi:10.1037//0021-9010.87.1.52
- Liden, R. C., & Maslyn, J. M. (1998). Multidimensionality of leader-member exchange: An empirical assessment through scale development. *Journal of Management*, 224(1), 43-72.
- Lin, C. P., Hung, W. T., & Chiu, C. K. (2008). Being good citizens: Understanding a mediating mechanism of organizational commitment and social network ties in OCBs. *Journal of Business Ethics*, 81(3), 561-578. doi:10.1007/s10551-007-9528-8
- Lindell, M. K., & Whitney, D. J. (2001). Accounting for Common Method Variance in Cross-sectional Research Designs. *Journal of Applied Psychology*, 86(1), 114-121.
- Lo, M. C., Ramayah, T., Min, H. W., & Songan, P. (2010). The relationship between leadership styles and organizational commitment in Malaysia: role of leader-member exchange. *Asia Pacific Business Review*, 16(1-2), 79-103. doi:10.1080/13602380903355676
- MacKenzie, S. B., Podsakoff, P. M., & Ahearne, M. (1998). Some possible antecedents and consequences of in-role and extra-role salesperson performance. *Journal of Marketing*, 62(3), 87-98. doi:10.2307/1251745
- Markham, S. E. (2012). The evolution of organizations and leadership from the ancient world to modernity: A multilevel approach to organizational science and leadership (OSL). *Leadership Quarterly*, 23(6), 1134-1151. doi:10.1016/j.lequa.2012.10.011
- Mayer, R. C., & Gavin, M. B. (2005). Trust in management and performance: Who minds the shop while the employees watch the boss? *Academy of Management Journal*, 48(5), 874-888.
- Mayer, R. C., & Schoorman, F. D. (1992). PREDICTING PARTICIPATION AND PRODUCTION OUTCOMES THROUGH A 2-DIMENSIONAL MODEL OF ORGANIZATIONAL COMMITMENT. *Academy of Management Journal*, 35(3), 671-684. doi:10.2307/256492
- McGregor, D. (1960). *The Human Side of Enterprise*. New York: McGraw-Hill.
- McKeen, J. D., & Smith, H. (1996). *Management challenges in IS : successful strategies and appropriate action*. Chichester ; New York: Wiley.
- Michael, J. H., Evans, D. D., Jansen, K. J., & Haight, J. M. (2005). Management commitment to safety as organizational support: Relationships with non-safety outcomes in wood manufacturing employees. *Journal of Safety Research*, 36(2), 171-179. doi:10.1016/j.jsr.2005.03.002
- Morrison, E. W. (1994). Role definitions and organizational citizenship behavior: The importance of the employee's perspective. *Academy of Management Journal*, 37(6), 1543-1567.
- Murphy, S. M., Wayne, S. J., Liden, R. C., & Erdogan, B. (2003). Understanding social loafing: The role of justice perceptions and exchange relationships. *Human Relations*, 56(1), 61-84.
- Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18(2), 126-139.
- Organ, D. W. (1988). *Organizational Citizenship Behavior: The Good Soldier Syndrome*. Lexington, MA: Lexington.

- Organ, D. W. (1990). THE MOTIVATIONAL BASIS OF ORGANIZATIONAL CITIZENSHIP BEHAVIOR. *Research in Organizational Behavior*, 12, 43-72.
- Organ, D. W. (1997). Organizational citizenship behavior: It's construct clean-up time. *Human Performance*, 10(2), 85-97. doi:10.1207/s15327043hup1002_2
- Organ, D. W., Podsakoff, P. M., & MacKenzie, S. B. (2006). *Organizational Citizenship Behavior: Its Nature, Antecedents, and Consequences*. Thousand Oaks: SAGE Publications.
- Organ, D. W., & Ryan, K. (1995). A meta-analytic review of attitudinal and dispositional predictors of organizational citizenship behavior. *Personnel Psychology*, 48(4), 775-802. doi:10.1111/j.1744-6570.1995.tb01781.x
- Parker, S. K., Williams, H. M., & Turner, N. (2006). Modeling the antecedents of proactive behavior at work. *Journal of Applied Psychology*, 91(3), 636-652. doi:10.1037/0021-9010.91.3.636
- Pavlou, P. A., Liang, H. G., & Xue, Y. J. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *Mis Quarterly*, 31(1), 105-136.
- Podsakoff, N. P., Whiting, S. W., Podsakoff, P. M., & Blume, B. D. (2009). Individual- and Organizational-Level Consequences of Organizational Citizenship Behaviors: A Meta-Analysis. *Journal of Applied Psychology*, 94(1), 122-141. doi:10.1037/a0013079
- Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of protection-motivated behaviors. *Mis Quarterly*, 37(4), 1189-1210.
- Rathnam, P. G., Johnsen, J., & Wen, H. J. (2004). Alignment of business strategy and it strategy: A case study of a fortune 50 financial services company. *Journal of Computer Information Systems*, 45(2), 1-8.
- Ringle, C. M., Wende, S., & Will, S. (2005). SmartPLS 2.0 (M3) Beta. Hamburg, Germany.
- Rizzo, J. R., House, R. J., & Lirtzman, S. I. (1970). Role conflict and ambiguity in complex organizations. *Administrative Science Quarterly*, 15(2), 150-163.
- Robinson, S. L., & Morrison, E. W. (1995). PSYCHOLOGICAL CONTRACTS AND OCB - THE EFFECT OF UNFULFILLED OBLIGATIONS ON CIVIC VIRTUE BEHAVIOR. *Journal of Organizational Behavior*, 16(3), 289-298. doi:10.1002/job.4030160309
- Romme, A. G. L. (1997). Work, authority and participation: The scenario of circular organizing. *Journal of Organizational Change Management*, 10(2), 156-+. doi:10.1108/09534819710160817
- Schuh, S. C., Zhang, X. A., & Tian, P. (2013). For the Good or the Bad? Interactive Effects of Transformational Leadership with Moral and Authoritarian Leadership Behaviors. *Journal of Business Ethics*, 116(3), 629-640. doi:10.1007/s10551-012-1486-0
- Seers, A. (1989). Team-member exchange quality: A new construct for role-making research. *Organizational Behavior and Human Decision Processes*, 43(1), 118-135.
- Shankar, A., Ansari, M. A., & Saxena, S. (1994). ORGANIZATIONAL CONTEXT AND INGRATIATORY BEHAVIOR IN ORGANIZATIONS. *Journal of Social Psychology*, 134(5), 641-647.
- Shore, L. M., Bommer, W. H., Rao, A. N., & Seo, J. (2009). Social and economic exchange in the employee-organization relationship: the moderating role of reciprocity wariness. *Journal of Managerial Psychology*, 24(7-8), 701-721. doi:10.1108/02683940910996752
- Shore, L. M., Tetrck, L. E., Lynch, P., & Barksdale, K. (2006). Social and economic exchange: Construct development and validation. *Journal of Applied Social Psychology*, 36(4), 837-867.
- Siponen, M., & Vance, A. (2010). Neutralization: New insight into the problem of employee information systems security policy violation. *MIS Quarterly*, 34(3), 487-502.
- Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security violations. *European Journal of Information Systems*, 23(3), 289-305.

- Solomon, M. R., Surprenant, C., Czepiel, J. A., & Gutman, E. G. (1985). A role theory perspective and dyadic interactions: The service encounter. *Journal of Marketing*, 49(1), 99 -111.
- Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employee's motivation to follow IS security policies. *Information & Management*, 48(7), 296-302.
- Song, L. J., Tsui, A. S., & Law, K. S. (2009). Unpacking Employee Responses to Organizational Exchange Mechanisms: The Role of Social and Economic Exchange Perceptions. *Journal of Management*, 35(1), 56-93. doi:10.1177/0149206308321544
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *Mis Quarterly*, 34(3), 503-522.
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *Mis Quarterly*, 22(4), 441-469.
- Sun, L. Y., Aryee, S., & Law, K. S. (2007). High-performance human resource practices, citizenship behavior, and organizational performance: A relational perspective. *Academy of Management Journal*, 50(3), 558-577.
- Thau, S., Bennett, R. J., Mitchell, M. S., & Marrs, M. B. (2009). How management style moderates the relationship between abusive supervision and workplace deviance: An uncertainty management theory perspective. *Organization Behavior and Human Decision Processes*, 108(1), 79-92.
- Trkman, P., & Desouza, K. C. (2012). Knowledge risks in organizational networks: An exploratory framework. *Journal of Strategic Information Systems*, 21, 1-17.
- Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52(4), 506-517. doi:<http://dx.doi.org/10.1016/j.im.2015.03.002>
- Turner, N., Chmiel, N., & Walls, M. (2005). Railing for safety: Job demands, job control, and safety citizenship role definition. *Journal of Occupational Health Psychology*, 10(4), 504-512.
- van Dyne, L., Cummings, L. L., & Parks, J. M. (1995). Extra-role behaviors: In pursuit of construct and definitional clarity (a bridge over muddied waters). In L. L. Cummings & B. M. Staw (Eds.), *Research in Organizational Behavior* (Vol. 17, pp. 215-285). Greenwich, CT: JAI Press.
- van Dyne, L., Graham, J. W., & Dienesch, R. M. (1994). ORGANIZATIONAL CITIZENSHIP BEHAVIOR - CONSTRUCT REDEFINITION, MEASUREMENT, AND VALIDATION. *Academy of Management Journal*, 37(4), 765-802.
- van Dyne, L., Kamdar, D., & Joireman, J. (2008). In-role perceptions buffer the negative impact of low LMX on helping and enhance the positive impact of high LMX on voice. *Journal of Applied Psychology*, 93(6), 1195-1207.
- Van Dyne, L., & LePine, J. A. (1998). Helping and voice extra-role behaviors: Evidence of construct and predictive validity. *Academy of Management Journal*, 41(1), 108-119.
- van Offenbeek, M., Boonstra, A., & Seo, D. (2013). Towards integrating acceptance and resistance research: evidence from a telecare case study. *European Journal of Information Systems*, 22(4), 434-454. doi:10.1057/ejis.2012.29
- Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3-4), 190-198.
- Wasko, M. M., & Faraj, S. (2000). "It is what one does": why people participate and help others in electronic communities of practice. *Journal of Strategic Information Systems*, 9(2-3), 155-173.
- Wat, D., & Shaffer, M. A. (2005). Equity and relationship quality influences on organizational citizenship behaviors - The mediating role of trust in the supervisor and empowerment. *Personnel Review*, 34(4), 406-422. doi:10.1108/00483480510599752
- Williams, K. D., & Sommer, K. (1997). Social ostracism by coworkers: Does rejection lead to loafing or compensation? *Personality and Social Psychology Bulletin*, 23(7), 693-706.

- Williams, L. J., & Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of Management*, 17(3), 601-617. doi:10.1177/014920639101700305
- Woller, K. M. P., Buboltz, W. C., & Loveland, J. M. (2007). Psychological reactance: Examination across age, ethnicity, and gender. *American Journal of Psychology*, 120(1), 15-24.
- Yu, C. P., & Chu, T. H. (2007). Exploring knowledge contribution from an OCB perspective. *Information & Management*, 44(3), 321-331. doi:10.1016/j.im.2007.03.002
- Zhang, A. Y., Tsui, A. S., & Wang, D. X. (2011). Leadership behaviors and group creativity in Chinese organizations: The role of group processes. *Leadership Quarterly*, 22(5), 851-862. doi:10.1016/j.lequa.2011.07.007
- Zhang, X., & Bartol, K. M. (2010). Linking empowering leadership and employee creativity: The influence of psychological empowerment, intrinsic motivation, and creative process engagement. *Academy of Management Journal*, 53(1), 107-128.

Figures

FIGURE 1: Research Model

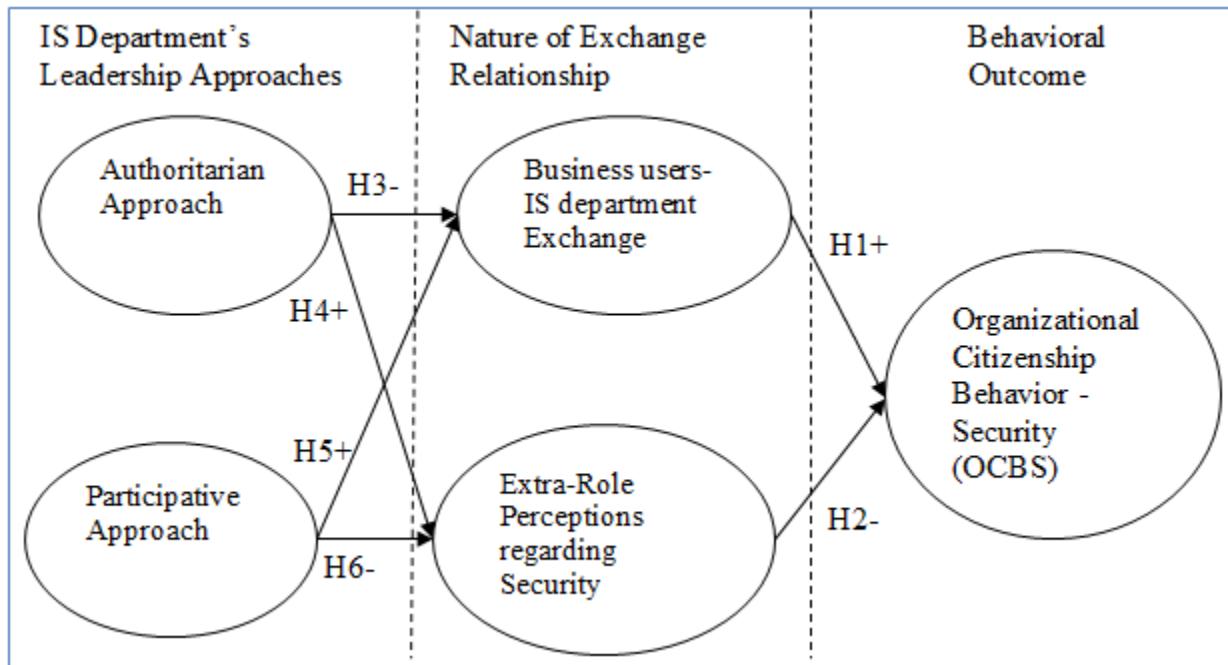
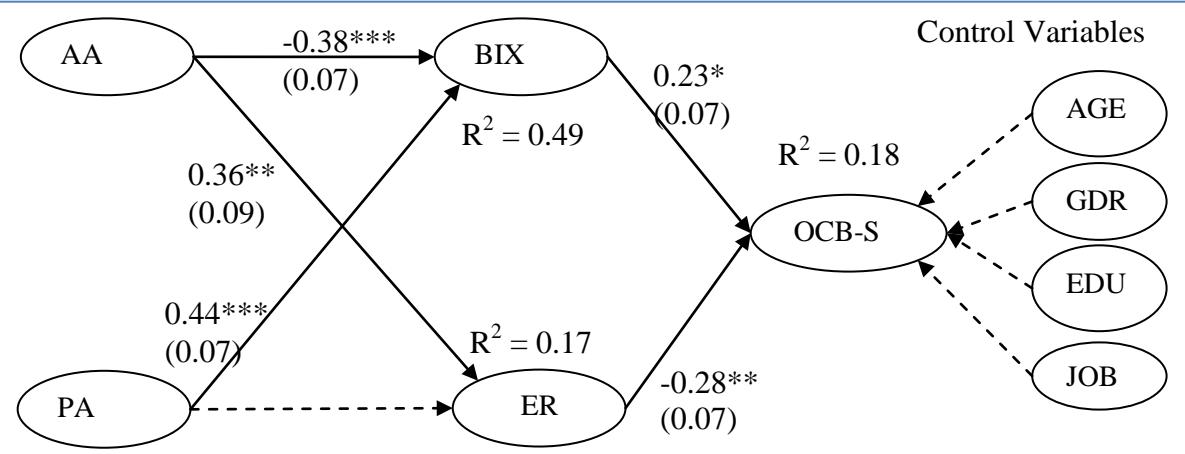


FIGURE 2: Results



Notes: (1) AA: Authoritarian Approach; PA: Participative Approach; BIX: Business users-IS department Exchange; ER: Extra-Role Perception; OCB-S: Organizational Citizenship Behavior regarding Security; GD: Gender; EDU: Education; JOB: Job Level. (2) Dotted lines represent non-significant paths. (3) *: $p < 0.05$; **: $p < 0.01$; ***: $p < 0.001$. (4) Standard errors in parentheses.

Organizational Citizenship Behavior regarding Security (OCB-S): Leadership Approach Perspective

Appendix 1: Detailed Theoretical Background

A1.1 OCB-S

A significant body of research in the IS security literature has been devoted to investigating why end-users violate or comply with organizational policies, or engage in security-related behaviors (D'Arcy & Herath, 2011; Guo, 2013b; Siponen & Vance, 2014). Many such studies have focused on negative and/or malicious IS security behaviors (such as policy violations and information systems misuse) while paid relatively less attention to positive and benevolent behaviors aimed at helping the organization maintain its information assets secure (Guo, 2013b; Hsu et al., 2015; Posey et al., 2013). In addition, the few studies on positive IS security behaviors (Guo, 2013b; Hsu et al., 2015; Posey et al., 2013), tended to focus on calculative compliance-based decisions that assume a rational desire to avoid punishment, rather than on relationship/leadership- and role-based decisions. The latter perspective may also be relevant and perhaps more appropriate in cases where sanctions and rewards are not tied to one's IS security performance; this is arguably the situation in many organizations.

In this study, we aim to partially fill this gap by focusing on relational- and role-based consideration in enacting positive IS security behaviors. To do so, we add to the limited body of research on benevolent IS security behaviors a special type of positive and benevolent behavior, which we call OCB-S. This concept is similar to other positive behaviors but is informed by a rich body of research in the management literature on OCB (Choi, 2007; Den Hartog, De Hoogh, & Keegan, 2007; Parker, Williams, & Turner, 2006). Tying into this well established research

stream can allow IS researchers to better theorize on and explain positive organizational behaviors in the domain of IS (Ifinedo, 2015).

The importance of OCB stems from that fact that it is often more potent compared to compliance behaviors in improving a range of organizational outcomes (Podsakoff et al., 2009). This happens because OCB is voluntary, above-and-beyond one's job duties, out of dedication, and organizationally- rather than self-focused(Organ et al., 2006). Specifically, when people engage in OCB, for example by helping others, improving their knowledge, or ensuring that others' comply with policies (Organ, 1988; Organ et al., 2006), organizational performance is improved (LePine et al., 2002; Morrison, 1994; Organ, 1997; Organ & Ryan, 1995; van Dyne, Graham, & Dienesch, 1994). This idea is also supported in the context of work safety, which has similar features to those presented by IS security (Hofmann & Morgeson, 1999; Hofmann, Morgeson, & Gerras, 2003; Michael, Evans, Jansen, & Haight, 2005; Turner, Chmiel, & Walls, 2005); when employees present safety-related citizenship behaviors, performance indicators are improved. In this regard, OCB-S is similar to OCB-safety in that it is a nuanced type of OCB (as opposed to general OCB) that can relatively proximally explain domain specific (security, safety, etc.) behaviors. Hence, increasing OCB-S may be a desirable organizational aim.

In this paper we rely on the OCB literature and define OCB-S as those intentional but voluntary actions that end-users carry out beyond their main job responsibilities in order to protect the organization's information systems and assets. The OCB literature suggests that OCB can be targeted toward the organization and directly benefit it (OCB-Organization; OCB-O, such as not taking breaks, showing pride in the organizations, conserving and protecting organizational property) or toward individuals (OCB-individual; OCB-I, including guiding others in the organization, being courteous to others, passing information to, listening to and helping other

employees)(L. J. Williams & Anderson, 1991). OCB related to IS security behaviors could fall in either category; employees can engage in above-duty behaviors that target coworkers (e.g., helping them to maintain information security) or the organization (e.g., suggesting improvements to information security). Hence, our measure of OCB-S taps into both aspects and one can view OCB-S as a contextualized OCB targeted at both individuals and the organization.

OCB-S is similar to what is referred to as security assurance behaviors (Guo, 2013b) and extra-role behaviors (Hsu et al., 2015). We choose to use the term OCB-S rather than other terms, because it is a more focused concept (e.g., it emphasizes specific security-targeted behaviors) and for the purpose of aligning it with the management literature and the theories we borrow from it in this study. Specifically, OCB-S can be seen as a nuanced category of protection-motivated behavior (Posey et al., 2013). The key characteristic of OCB-S is that it is often voluntary as opposed to required or even expected by the organization, typically executed out of dedication rather than out of constraint, and is not perceived as being a key integral part of a person's job definition. Ultimately, it is not a direct component in employees' job performance (Organ et al., 2006). IS Security is often seen as non-user task (Besnard & Arief, 2004). Thus from the organizational IS security management perspective, end-users who comply with policies are doing what they are expected to do, often in order to avoid punishment (Chen, Ramamurthy, & Wei, 2012; D'Arcy et al., 2009; Herath & Rao, 2009b). In contrast, employees engaging in OCB-S, for instance by motivating other employees to engage in IS security behaviors or by making suggestions to improve information security, are going above and beyond what they are expected to do, not necessarily to improve their own evaluation of performance, but rather to help others and the organization. Furthermore, their motivations to do so can differ from those driving other positive information security behaviors. For instance,

OCB-S can stem from relational reciprocity (Eisenberger et al., 2001; L. M. Shore et al., 2009) rather than from self-benefit promotion or punishment-avoidance considerations (Chen et al., 2012).

These attributes of OCB-S make it an important concept with many possible positive impacts on organizations. Borrowing from the OCB literature, such effects may include increased trust, participation, work performance and improved attitudes, compared with in-role-related “forced” behaviors (Aryee, Budhwar, & Chen, 2002; Mayer & Schoorman, 1992; Organ, 1988; Organ, 1997; Organ et al., 2006). Furthermore, citizenship behaviors emerge from antecedents that differ from those driving role-related, less voluntary, more self-focused, and less proactive behaviors (Organ, 1990; Organ et al., 2006). Hence, we focus on OCB-S, as well as on its unique relational predictors in this study.

A1.2 Authoritarian and Participative Approaches of Management

We draw upon relevant theories in the management literature to conceptualize the ways in which IS departments may manage their relationships with end-users and govern, at least in part, IS projects. As mentioned earlier, while IS departments are typically not the sole leader of IS projects, they do provide leadership, at least regarding technical matters, in all IS projects (Banker et al., 2011). Work units typically have different prototypical leadership approaches for interacting with their constituents (Hambley, O'Neill, & Kline, 2007; Kahai, Sosik, & Avolio, 1997). At one extreme is the authoritarian approach, which is also referred to as Theory X (McGregor, 1960) and coercive formalization (Adler & Borys, 1996). This approach assumes that employees must be controlled and directed by rules and procedures; and employees will be punished if they fail to follow rules and procedures (an economic-exchange approach). At the other extreme is the participative approach, which is also referred to as Theory Y (McGregor,

1960) and enabling formalization (Adler & Borys, 1996). This approach assumes that constituents are motivated and self-directed without control and punishment; and constituents (employees, clients, co-workers) take active roles in the design and continuous improvement of business processes, including presumably IS security.

The participative approach often leads to positive results; it can improve employee attitudes, and increase perceived social pressure and perceived capability to take initiative to improve performance (Groen, Wouters, & Wilderom, 2012). In contrast, the authoritarian approach results in disciplined behavior, but often diminishes extra role behaviors (Schuh, Zhang, & Tian, 2013).

It should be noted that these prototypical approaches are not mutually exclusive; managers often employ some aspects of the authoritarian approach together with others of the participative approach, and they may use different approaches in different situations – equally likely, or one more frequently than the other (Aycan, Schyns, Sun, Felfe, & Saher, 2013; Chakravarthy & Gargiulo, 1998; Romme, 1997; Shankar, Ansari, & Saxena, 1994). In fact, to get the best results, people are encouraged to rotate between and engage in all types of management approaches, depending on the situations they face (Goleman, 2000). Hence, we expect IS departments in our study to present some degree of each one of these approaches.

The authoritarian and participative leadership ideas can be applied to security management practices, because centralized IS departments often use various leadership tactics to convince users (who typically do not report to the IS department) to engage in what they perceive to be desirable or appropriate security behaviors (Fuchs, Pernul, & Sandhu, 2011; Spears & Barki, 2010). Most likely, IS leaders are not different from the rest in that they simultaneously employ

different approaches, or rotate between different approaches in a contingent manner, i.e., based on the situation (Goleman, 2000). Hence, it is expected that they employ different degrees of authoritarian and participative approaches when developing, conveying and implementing IS security policies.

An authoritarian approach to security management usually treats end-users as insider threats or potential enemies to security (Adams & Sasse, 1999). To deal with such threats, the organization, often through the IS department (Straub & Welke, 1998), implements strict security policies that aim to regulate how end-users use information systems; end-users who fail to follow the policies would be punished and are often not involved in developing these policies. This approach entails a need-to-know principle in that end-users need to know no more than what is necessary regarding security and their duties, and they are expected to follow well-structured security management guidelines developed by experts (the IS department) or implicit organizational expectations (Chen et al., 2012; Herath & Rao, 2009b). An example of this approach would be a directive without explanations from the IS department regarding a need to change the password every three months.

In contrast to the authoritarian approach, a participative approach to security management does not assume that end-users are potential enemies. Instead, it suggests that end-users should be treated as partners and knowledge resources for IS security management (Adams & Blandford, 2005; Adams & Sasse, 1999; Albrechtsen & Hovden, 2009; Dourish et al., 2004; Hedström, Kolkowska, Karlsson, & Allen, 2011; Spears & Barki, 2010). This approach entails the interaction and collaboration between end-users and the IS department; security procedures are designed and implemented with end-users' participation and inputs, and would leave end-users at least some control over their security behaviors. An example of this approach would be a

committee that includes IS department employees and end-users that discuss the right balance between security needs and performance and employee satisfaction tradeoffs.

A1.3 Social Exchange Theory and Role Theory

To examine the influence of IS security management on end-user OCB-S, we apply social exchange theory and roles theory as an overarching theoretical framework. Social exchange theory (Blau, 1964) builds on the principle of reciprocity in that “an individual who supplies rewarding services to another obligate him. To discharge this obligation, the second must furnish benefits to the first in turn.” There are two key types of exchange relationship: social exchange and economic exchange. Social exchange refers to “voluntary actions of individuals that are motivated by the returns they are expected to bring.” A crucial characteristic of social exchange is unspecified obligations. Thus, social exchange focuses on long-term relationships and the social-emotion aspects of the relationship (L.M. Shore et al., 2006).

Social exchange theory has been applied in a variety of management contexts. In organizational settings, employees work in a social environment in which they interact with each other to perform business tasks. Thus their relationships with coworkers, supervisors, and management will likely have impact on their job performance and daily lives. Bad relationships may turn into social ostracism (the perception of being ignored by others) that can have strong negative behavioral and emotional consequences (K. D. Williams & Sommer, 1997). Two specific types of relationship have drawn much attention in the management literature. One is the relationship between employees and leaders. This type of relationship has been referred to as leader-member exchange (LMX), defined as the reciprocal exchanges between employees and their direct or indirect supervisors based on trust, respect, and obligations (Graen & Uhl-Bien, 1995). The other type of relationship is between employees and their coworkers. This type of relationship is

referred to as team-member exchange (TMX), defined as employees' social exchanges with coworkers in terms of the reciprocal contribution of ideas, feedback, and assistance (Seers, 1989).

It is generally accepted that high quality relationships will lead to favorable outcomes whereas low quality relationships will lead to unfavorable outcomes. For example, a recent meta-analysis found that employee perceptions of LMX are positively related to job performance and organizational citizenship behavior and are negatively related to turnover intentions (Dulebohn, Bommer, Liden, Brouer, & Ferris, 2012). Other studies have found evidence supporting the effects of LMX and/or TMX on a variety of outcomes such as helping behavior (Kamdar & van Dyne, 2007), social loafing (Murphy, Wayne, Liden, & Erdogan, 2003), and job attitudes (Seers, 1989). In essence, employees in better work relationships tend to be more willing to do something in return for the other parties in the relationships.

In contrast to social exchange, economic exchange rests on a formal contract that stipulates what exactly are to be exchanged (Blau, 1964). In an organizational setting, employees perceive their relationship with their employer by incorporating financial and material obligations in exchange for their fulfillment of job duties (or their role responsibilities as specified in their employment contracts) when high levels of economic exchange are present (L.M. Shore et al., 2006). Thus from this perspective, the concept of economic exchange is consistent with role theory.

According to role theory (Biddle, 1979), roles coordinate and guide employees in terms of how roles should be performed. Roles, which are defined as the set of expected activities for specific job positions, delineate expected behaviors and responsibilities; they form the foundation of job descriptions, expectations and stereotypes (Dierdorff, Rubin, & Bachrach, 2012; van Dyne,

Cummings, & Parks, 1995; van Dyne et al., 2008). Role perceptions are important because they influence employee behaviors (Biddle, 1979; Solomon, Surprenant, Czepiel, & Gutman, 1985).

A body of research in the management literature has focused on the effects of in-role and extra-role perceptions. Prior research has found that employees will be more likely to engage in certain behaviors if they view the behavior as in-role (i.e. part of their roles) rather than extra-role (i.e. not part of their roles). For example, the more broadly employees define their job responsibilities, the more likely they will engage in organizational citizenship behavior (e.g. helping co-workers even when not asked)(Morrison, 1994). Conversely, people maintain their efforts invested in task-related aspects of the job but reduce their investment in activities that are perceived as extra-role (Haun, Steinmetz, & Dormann, 2011).

We argue that social and economic exchange relationships are two important aspects of IS security management in organizations. IS departments rely on end-users to carry out security tasks when they use technology in their business activities. Employees typically do not report to the IS department. However, they may be sanctioned to engage in certain security behaviors. Hence, there is a complex relationship between the IS department and users, the quality of which can determine above-duty positive IS security behaviors. Thus social exchange theory and role theory can be a useful lens for examining the effects of security management practices and consequent relational and job perception facets on user OCB-S.

Appendix 2: Measurement Scale

The suggested model was tested with data collected in China with a paper-based survey administered to employees of firms with whom the researchers had professional contacts. To develop measurement scales, we searched relevant literature for existing scales, which were then

adapted to reflect the security context. More specifically, *authoritarian approach (AA)* is adapted from (Thau, Bennett, Mitchell, & Marrs, 2009); *participative approach (PA)* is adapted from (X. Zhang & Bartol, 2010); *business users -IS department exchange (BIX)* is adapted from (Graen & Uhl-Bien, 1995; Liden & Maslyn, 1998); *extra-role perceptions regarding IS security (ER)* is adapted from (Rizzo, House, & Lirtzman, 1970); and *organizational citizenship behavior regarding security (OCB-S)* is adapted from (Turner et al., 2005).

As the original scales were in English, we further performed a number of adaptation steps to ensure measurement equivalence (Farh, Cannella, & Lee, 2006). First, we reviewed the English scales and tried to make necessary revisions to reflect the Chinese context. Second, bilingual professionals independently translated the scales into Chinese. The translated versions of the scales were then compared and discussed by the two bilingual authors until all major discrepancies were eliminated. Third, we took a “cooling-off” period of about one month and then came back to take a fresh look at the scales. We paid particular attention to eliminate potential ambiguity that may arise in translating measurement items from Chinese to English. Some further minor revisions were made based on the fresh review. Lastly, we conducted a pilot study by administering the survey to a group of 64 end-users (employees of a large electronics retailer in China and full-time MBA students in China). The results suggested that the scales are sufficiently valid and reliable (Composite Reliability scores ranged from 0.9 to 0.94; loadings were over 0.7 and significant and cross-loadings were small and below 0.35). Minor revisions were made based on feedback from pilot-study participants.

All measurement items use a Likert scale of 1 (strongly disagree or least likely) to 7 (strongly agree or most likely). Scales are given in Table A2.1.

A2.1: Scales

Construct [Acronym] (Source/s)	Items
Authoritarian Approach [AA] (Thau et al., 2009)	<ul style="list-style-type: none"> - The IS department is domineering in the sense of trying to impose too much control on computer use. - The IS people have difficult time seeing our points of view. - The IS department hammers down strict rules that waste our time and resources. - The IS department uses many unreasonable rules that impede our work. - The IS department often treats us as trouble-makers.
Participative Approach [PA] (X. Zhang & Bartol, 2010)	<ul style="list-style-type: none"> - The IS department often consults us on important IS decisions. - The IS department often solicits our opinions on IS decisions that may affect our work. - The IS department often treat supporting our work as a priority - The IS department takes our opinion seriously. - The IS department often helps us to solve computer problems.
Business Users -IS Department Exchange [BIX] (Graen & Uhl-Bien, 1995; Liden & Maslyn, 1998)	<ul style="list-style-type: none"> - IS people in the organization understand my job problems and needs. - IS people in the organization are always available to help me solve my computer problems. - I have enough confidence in IS people in the organization. - I have a good working relationship with IS people in the organization. - I respect the organization's IS people knowledge of and competence in their job. - I do not mind doing a favor in return for IS people in the organization.
Extra-Role Perceptions regarding IS Security [ER] (Rizzo et al., 1970)	<ul style="list-style-type: none"> - I do not have any time and resources to care about information security. - Information security is not part of my job. - Information security problems are beyond my job responsibility. - Information security is IS people's job, not mine.
Organizational Citizenship Behavior – Security [OCB-S] (Turner et al., 2005)	<p>How likely would you do the following (1=least likely; 7=most likely)</p> <ul style="list-style-type: none"> - Telling coworkers to follow security rules and procedures. - Doing something to stop insecure use of computers. - Making suggestions to improve information security. - Keeping informed of security rules and procedures.

Appendix 3: Data Collection and Sample

The survey was distributed to 260 end-users in select companies located in China. These companies were from various industries such as online retail, manufacturing, product inspection

services, and telecommunication. The key criteria for company selection were: (1) the use of information systems for supporting critical business processes, (2) security is a key element of IS management for the organization, and (3) the existence of a central IS department. The surveys were distributed to end-users in these firms (after receiving permission from the CEOs), and collected directly by the research team without the intervention of management at each location. Survey participants were assured that the survey was voluntary and anonymous and that management would not have access to individual surveys. These efforts yielded 223 valid responses. The response rate (85.8%) was relatively higher than typical IS research. There are two plausible reasons. On the one hand, the survey was paper-based. This format allowed face-to-face interaction between participants and the researchers, thereby alleviating the delete-without-reading problem in email surveys. On the other hand, the survey was distributed with permission from those sampled companies, and was endorsed by the companies' CEOs. Thus participants did not worry about any potential problems that may result from them talking about internal organizational issues with external parties (i.e. the researchers) and may have felt somewhat obliged to complete the surveys given the CEO's endorsement.

The respondents were, on average, 33 years old (median 30), and 91% of them had college education. About 80% of the respondents classified themselves as "staff" as opposed to having supervisory responsibilities (mid-level and senior-level managers), and about 56% of the respondents were female. Additional demographic information is shown in Table A3.1.

TABLE A3.1: Demographic Profile of Respondents

Category	Measures	Count	Percentage (%)
----------	----------	-------	----------------

Age	< 24 25 – 34 35 - 44 44-55 > 55	25 127 36 30 5	21.7 57.5 14.0 4.8 1.4
Gender	Male Female	125 98	56.1 43.9
Education	High school Undergraduate Graduate Doctoral	21 183 17 2	9.4 82.1 7.6 0.9
Job Title	High Level Manager Middle Level Manager Employee Others	1 42 179 1	0.4 18.8 80.3 0.4
Computer usage (hours per day)	< 2 2-4 4-6 6-8 8-10 > 10	5 7 28 124 46 13	2.2 3.1 12.6 55.6 20.6 5.9

Note: N = 223

Appendix 4: Preliminary Scale Assessments

A4.1 Common Method Bias Risk Assessment

We took two approaches to address possible bias in our data. First, we examined the correlation matrix and detected no excessively large correlations, which would be indicative of potential common method variance; in addition some of the correlations were positive and others negative (Pavlou, Liang, & Xue, 2007). Second, an external marker construct, techno-stress (Ayyagari, Grover, & Purvis, 2011), was added to a confirmatory factor analysis model including all the model's constructs, as per Lindell and Whitney (2001). This marker variable had high loadings on its items (>0.75), and low cross loadings on the model's constructs (< 0.23). In addition, it had low and non-significant correlations with some of the model's constructs, e.g., with OCB-S

($r=0.01$, ns). The results of these tests therefore indicate that common method variance is unlikely to be influential in our data.

A4.2 Measurement Model

As shown in Table A4.2.1, the square root of average variance extracted (AVE) and the composite reliabilities of all constructs exceeded common thresholds. Moreover, all item loadings were greater than 0.70 (See Table A4.2.1). Hence, acceptable convergent validity was achieved (Fornell & Larcker, 1981). Similarly, sufficient discriminant validity was demonstrated by the relatively large differences between the AVE of a construct and construct correlations with other constructs (see Table A.4.2.2), as well as by large differences between loadings and cross-loadings. We further tested the discriminant validity of the two leadership approaches by using principal component analysis in SPSS 24. The analysis produced the two expected factors with loadings >0.7 and cross loadings <0.3 . Furthermore, the correlation between the constructs was relatively low (-0.475).

TABLE A4.2.1: Loadings and cross-loadings

Indicator	AA	BIX	ER	PA	OCB-S
AA1	<u>0.905</u>	-0.517	0.362	-0.412	-0.344
AA2	<u>0.925</u>	-0.548	0.404	-0.450	-0.333
AA3	<u>0.925</u>	-0.531	0.337	-0.436	-0.266
AA4	<u>0.916</u>	-0.509	0.360	-0.448	-0.285
AA5	<u>0.889</u>	-0.569	0.364	-0.419	-0.279
BIX1	-0.377	<u>0.753</u>	-0.177	0.484	0.165
BIX2	-0.565	<u>0.907</u>	-0.208	0.565	0.259
BIX3	-0.569	<u>0.900</u>	-0.167	0.556	0.259
BIX4	-0.533	<u>0.900</u>	-0.180	0.552	0.258
BIX5	-0.514	<u>0.859</u>	-0.184	0.512	0.342
BIX6	-0.410	<u>0.774</u>	-0.185	0.491	0.214
ER1	0.372	-0.194	<u>0.821</u>	-0.252	-0.280
ER2	0.331	-0.190	<u>0.912</u>	-0.188	-0.312
ER3	0.359	-0.171	<u>0.924</u>	-0.246	-0.282
ER4	0.376	-0.213	<u>0.927</u>	-0.251	-0.346
PA1	-0.305	0.382	-0.206	<u>0.803</u>	0.276

PA2	-0.383	0.430	-0.246	<u>0.849</u>	0.275
PA3	-0.425	0.568	-0.238	<u>0.923</u>	0.274
PA4	-0.447	0.610	-0.262	<u>0.935</u>	0.307
PA5	-0.455	0.615	-0.178	<u>0.792</u>	0.272
OCB-S1	-0.260	0.272	-0.245	0.282	<u>0.852</u>
OCB-S2	-0.273	0.297	-0.307	0.310	<u>0.908</u>
OCB-S3	-0.298	0.211	-0.317	0.298	<u>0.896</u>
OCB-S4	-0.334	0.265	-0.331	0.262	<u>0.878</u>

Notes: (1) AA: Authoritarian Approach; PA: Participative Approach; BIX: Business users-IS department Exchange; ER: Extra-Role Perception; OCB-S: Organizational Citizenship Behavior - Security. (2) Underlined numbers are factor loadings. A list of indicators can be found in Appendix 2.

TABLE A4.2.2: Descriptive Statistics, AVE, Composite Reliability, and Construct Correlations

Construct	Mean (Std. Dev.)	Average Variance Extracted	Composite Reliability	AA	BIX	ER	PA	OCB-S
AA	3.09 (1.63)	0.832	0.961	<u>0.912</u>				
BIX	5.31 (1.25)	0.724	0.940	-0.587	<u>0.851</u>			
ER	3.00 (1.73)	0.805	0.943	0.402	-0.215	<u>0.897</u>		
PA	4.57 (1.54)	0.744	0.935	-0.475	0.619	-0.262	<u>0.863</u>	
OCB-S	4.94 (1.58)	0.781	0.934	-0.331	0.297	-0.341	0.325	<u>0.884</u>

Notes: (1) AA: Authoritarian Approach; PA: Participative Approach; BIX: Business users-IS department Exchange; ER: Extra-Role Perception; OCB-S: Organizational Citizenship Behavior - Security. (2) Underlined numbers on diagonal are the square roots of AVE (average variance extracted).

Appendix 5: Post-hoc Analyses

We also calculated effect sizes for the exogenous constructs (AA, PA) in predicting the endogenous constructs (BIX, ER, OCB-S). As shown in Table 3, the effect size ranged from 0.07 to 0.31, reflecting small to large effects based on the Cohen criteria (Cohen, 1992).

Table 3. Effect Sizes

Path	Effect Size
AA -> BIX	0.23
AA -> ER	0.13
BIX -> OCB-S	0.07

ER -> OCB-S	0.11
PA -> BIX	0.31

We obtained additional indices to assess model fitness by using SmartPLS 3: SRMR (Standardized Root Mean Square Residual)=0.04; NFI (Normed Fit Index)=0.90; RMS_theta (root mean squared residual covariance matrix of the outer model residuals)=0.16. These indices reflect a mixed a picture of model fit according to some generally accepted criteria (SRMR<0.10; NFI>0.90; RMS_Theta<0.12). It should be noted that PLS-SEM is designed for prediction purposes and the above indices should be interpreted accordingly, as other aspect of model quality, such as r-square, are more important in PLS analysis (Hair Jr, Hult, Ringle, & Sarstedt, 2017).

References

- Adams, A., and Blandford, A. 2005. "Bridging the gap between organizational and user perspectives of security in the clinical domain," *International Journal of Human-Computer Studies* (63:1-2), pp 175-202.
- Adams, A., and Sasse, M. A. 1999. "Users are not the enemy," *Communications of the ACM* (42:12), pp 41-46.
- Adler, P. S., and Borys, B. 1996. "Two types of bureaucracy: Enabling and coercive," *Administrative Science Quarterly* (41:1), pp 61-89.
- Albrechtsen, E., and Hovden, J. 2009. "The information security digital divide between information security managers and users," *Computers & Security* (28:6), pp 476-490.
- Aryee, S., Budhwar, P. S., and Chen, Z. X. 2002. "Trust as a mediator of the relationship between organizational justice and work outcomes: test of a social exchange model," *Journal of Organizational Behavior* (23:3) May, pp 267-285.
- Aycan, Z., Schyns, B., Sun, J. M., Felfe, J., and Saher, N. 2013. "Convergence and divergence of paternalistic leadership: A cross-cultural investigation of prototypes," *Journal of International Business Studies* (44:9) Dec, pp 962-969.
- Ayyagari, R., Grover, V., and Purvis, R. 2011. "Technostress: Technological antecedents and implications," *MIS Quarterly* (35:4) Dec, pp 831-858.
- Banker, R. D., Hu, N., Pavlou, P. A., and Luftman, J. 2011. "CIO reporting structure, strategic positioning, and firm performance," *MIS Quarterly* (35:2) Jun, pp 487-504.
- Besnard, D., and Arief, B. 2004. "Computer security impaired by legitimate users," *Computers & Security* (23:3), pp 253-264.
- Biddle, B. J. 1979. *Role Theory: Expectations, Identities, and Behaviors*, (Academic Press: New York.

- Blau, P. M. 1964. *Exchange and Power in Social Life*, (Wiley: New York, NY.
- Chakravarthy, B., and Gargiulo, M. 1998. "Maintaining leadership legitimacy in the transition to new organizational forms," *Journal of Management Studies* (35:4) Jul, pp 437-456.
- Chen, Y., Ramamurthy, K., and Wei, K.-W. 2012. "Organizations' information security policy compliance: Stick or carrot approach?," *Journal of Management Information Systems* (29:3), pp 157-188.
- Choi, J. N. 2007. "Change-oriented organizational citizenship behavior: effects of work environment characteristics and intervening psychological processes," *Journal of Organizational Behavior* (28:4) May, pp 467-484.
- Cohen, J. 1992. "A power primer," *Psychological Bulletin* (112:1), pp 155-159.
- D'Arcy, J., and Herath, T. 2011. "A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings," *European Journal of Information Systems* (20:6), pp 643-658.
- D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1) Mar, pp 79-98.
- Den Hartog, D. N., De Hoogh, A. H. B., and Keegan, A. E. 2007. "The interactive effects of belongingness and charisma on helping and compliance," *Journal of Applied Psychology* (92:4) Jul, pp 1131-1139.
- Dierdorff, E. C., Rubin, R. S., and Bachrach, D. G. 2012. "Role expectations as antecedents of citizenship and the moderating effects of work context," *Journal of Management* (38:2), pp 573-598.
- Dourish, P., Grinter, R. E., de la Flor, R. D., and Joseph, M. 2004. "Security in the wild: User strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing* (8:6), pp 391-401.
- Dulebohn, J. H., Bommer, W. H., Liden, R. C., Brouer, R. L., and Ferris, G. R. 2012. "A meta-analysis of antecedents and consequences of leader-member exchange: Integrating the past with an eye toward the future," *Journal of Management* (38:6), pp 1715-1759.
- Eisenberger, R., Armeli, S., Rexwinkel, B., Lynch, P. D., and Rhoades, L. 2001. "Reciprocal of perceived organizational support," *Journal of Applied Psychology* (86:1) Feb, pp 42-51.
- Farh, J., Cannella, A. A., and Lee, C. 2006. "Approaches to scale development in Chinese management research," *Management and Organization Review* (2:3), pp 301-318.
- Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp 39-50.
- Fuchs, L., Pernul, G., and Sandhu, R. 2011. "Roles in information security - A survey and classification of the research area," *Computers & Security* (30:8) Nov, pp 748-769.
- Goleman, D. 2000. "Leadership that gets results," *Harvard Business Review* (78:2) Mar-Apr, pp 78-+.
- Graen, G. B., and Uhl-Bien, M. 1995. "Relationship-based approach to leadership: Development of leader-member exchange (LMX) theory of leadership over 25 years: Applying a multi-level multi-domain perspective," *Leadership Quarterly* (6:2), pp 219-247.
- Groen, B. A. C., Wouters, M. J. F., and Wilderom, C. P. M. 2012. "Why do employees take more initiatives to improve their performance after co-developing performance measures? A field study," *Management Accounting Research* (23:2), pp 120-141.
- Guo, K. H. 2013. "Security-related behavior in using information systems in the workplace: A review and synthesis," *Computers & Security* (32), pp 242-251.
- Hair Jr, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2017. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, (SAGE Publications: Thousand Oaks, CA.
- Hambley, L. A., O'Neill, T. A., and Kline, T. J. B. 2007. "Virtual team leadership: The effects of leadership style and communication medium on team interaction styles and outcomes," *Organizational Behavior and Human Decision Processes* (103:1) May, pp 1-20.

- Haun, S., Steinmetz, H., and Dormann, C. 2011. "Objective work–nonwork conflict: From incompatible demands to decreased work role performance," *Journal of Vocational Behavior* (79:2), pp 578-587.
- Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J. P. 2011. "Value conflicts of information security management," *Journal of Strategic Information Systems* (20:4), pp 373-384.
- Herath, T., and Rao, H. R. 2009. "Protection motivation and deterrence: A framework for security policy compliance in organizations," *European Journal of Information Systems* (18:2), pp 106-125.
- Hofmann, D. A., and Morgeson, F. P. 1999. "Safety-related behavior as a social exchange: The role of perceived organizational support and leader-member exchange," *Journal of Applied Psychology* (84:2) Apr, pp 286-296.
- Hofmann, D. A., Morgeson, F. P., and Gerras, S. J. 2003. "Climate as a moderator of the relationship between leader-member exchange and content specific citizenship: Safety climate as an exemplar," *Journal of Applied Psychology* (88:1) Feb, pp 170-178.
- Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. 2015. "The role of extra-role behaviors and social controls in information security effectiveness," *Information Systems Research* (26:2), pp 282-300.
- Ifinedo, P. Year. "Effects of Organizational Citizenship Behavior and Social Cognitive Factors on Employees' NonMalicious Counterproductive Computer Security Behaviors: An Empirical Analysis" International Conference on Information Resource Management, AIS2015, pp. 1-13.
- Kahai, S. S., Sosik, J. J., and Avolio, B. J. 1997. "Effects of leadership style and problem structure on work group process and outcomes in an electronic meeting system environment," *Personnel Psychology* (50:1) Spr, pp 121-146.
- Kamdar, D., and van Dyne, L. 2007. "The joint effects of personality and workplace social exchange relationships in predicting task performance and citizenship performance," *Journal of Applied Psychology* (92:5), pp 1286-1298.
- LePine, J. A., Erez, A., and Johnson, D. E. 2002. "The nature and dimensionality of organizational citizenship behavior: A critical review and meta-analysis," *Journal of Applied Psychology* (87:1) Feb, pp 52-65.
- Liden, R. C., and Maslyn, J. M. 1998. "Multidimensionality of leader-member exchange: An empirical assessment through scale development," *Journal of Management* (224:1), pp 43-72.
- Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-sectional Research Designs," *Journal of Applied Psychology* (86:1), pp 114-121.
- Mayer, R. C., and Schoorman, F. D. 1992. "PREDICTING PARTICIPATION AND PRODUCTION OUTCOMES THROUGH A 2-DIMENSIONAL MODEL OF ORGANIZATIONAL COMMITMENT," *Academy of Management Journal* (35:3) Aug, pp 671-684.
- McGregor, D. 1960. *The Human Side of Enterprise*, (McGraw-Hill: New York.
- Michael, J. H., Evans, D. D., Jansen, K. J., and Haight, J. M. 2005. "Management commitment to safety as organizational support: Relationships with non-safety outcomes in wood manufacturing employees," *Journal of Safety Research* (36:2), pp 171-179.
- Morrison, E. W. 1994. "Role definitions and organizational citizenship behavior: The importance of the employee's perspective," *Academy of Management Journal* (37:6), pp 1543-1567.
- Murphy, S. M., Wayne, S. J., Liden, R. C., and Erdogan, B. 2003. "Understanding social loafing: The role of justice perceptions and exchange relationships," *Human Relations* (56:1), pp 61-84.
- Organ, D. W. 1988. *Organizational Citizenship Behavior: The Good Soldier Syndrome*, (Lexington: Lexington, MA.
- Organ, D. W. 1990. "THE MOTIVATIONAL BASIS OF ORGANIZATIONAL CITIZENSHIP BEHAVIOR," *Research in Organizational Behavior* (12), pp 43-72.

- Organ, D. W. 1997. "Organizational citizenship behavior: It's construct clean-up time," *Human Performance* (10:2), pp 85-97.
- Organ, D. W., Podsakoff, P. M., and MacKenzie, S. B. 2006. *Organizational Citizenship Behavior: Its Nature, Antecedents, and Consequences*, (SAGE Publications: Thousand Oaks).
- Organ, D. W., and Ryan, K. 1995. "A meta-analytic review of attitudinal and dispositional predictors of organizational citizenship behavior," *Personnel Psychology* (48:4) Win, pp 775-802.
- Parker, S. K., Williams, H. M., and Turner, N. 2006. "Modeling the antecedents of proactive behavior at work," *Journal of Applied Psychology* (91:3) May, pp 636-652.
- Pavlou, P. A., Liang, H. G., and Xue, Y. J. 2007. "Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective," *MIS Quarterly* (31:1), pp 105-136.
- Podsakoff, N. P., Whiting, S. W., Podsakoff, P. M., and Blume, B. D. 2009. "Individual- and Organizational-Level Consequences of Organizational Citizenship Behaviors: A Meta-Analysis," *Journal of Applied Psychology* (94:1) Jan, pp 122-141.
- Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of protection-motivated behaviors," *MIS Quarterly* (37:4), pp 1189-1210.
- Rizzo, J. R., House, R. J., and Lirtzman, S. I. 1970. "Role conflict and ambiguity in complex organizations," *Administrative Science Quarterly* (15:2), pp 150-163.
- Romme, A. G. L. 1997. "Work, authority and participation: The scenario of circular organizing," *Journal of Organizational Change Management* (10:2), pp 156-+.
- Schuh, S. C., Zhang, X. A., and Tian, P. 2013. "For the Good or the Bad? Interactive Effects of Transformational Leadership with Moral and Authoritarian Leadership Behaviors," *Journal of Business Ethics* (116:3) Sep, pp 629-640.
- Seers, A. 1989. "Team-member exchange quality: A new construct for role-making research" *Organizational Behavior and Human Decision Processes* (43:1), pp 118-135.
- Shankar, A., Ansari, M. A., and Saxena, S. 1994. "ORGANIZATIONAL CONTEXT AND INGRATIATORY BEHAVIOR IN ORGANIZATIONS," *Journal of Social Psychology* (134:5) Oct, pp 641-647.
- Shore, L. M., Bommer, W. H., Rao, A. N., and Seo, J. 2009. "Social and economic exchange in the employee-organization relationship: the moderating role of reciprocity wariness," *Journal of Managerial Psychology* (24:7-8), pp 701-721.
- Shore, L. M., Tetrick, L. E., Lynch, P., and Barksdale, K. 2006. "Social and economic exchange: Construct development and validation," *Journal of Applied Social Psychology* (36:4), pp 837-867.
- Siponen, M., and Vance, A. 2014. "Guidelines for improving the contextual relevance of field surveys: The case of information security violations," *European Journal of Information Systems* (23:3), pp 289-305.
- Solomon, M. R., Surprenant, C., Czepiel, J. A., and Gutman, E. G. 1985. "A role theory perspective and dyadic interactions: The service encounter," *Journal of Marketing* (49:1) Winter, pp 99 -111.
- Spears, J. L., and Barki, H. 2010. "User participation in information systems security risk management," *MIS Quarterly* (34:3), pp 503-522.
- Straub, D. W., and Welke, R. J. 1998. "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly* (22:4) Dec, pp 441-469.
- Thau, S., Bennett, R. J., Mitchell, M. S., and Marrs, M. B. 2009. "How management style moderates the relationship between abusive supervision and workplace deviance: An uncertainty management theory perspective," *Organization Behavior and Human Decision Processes* (108:1), pp 79-92.
- Turner, N., Chmiel, N., and Walls, M. 2005. "Railing for safety: Job demands, job control, and safety citizenship role definition," *Journal of Occupational Health Psychology* (10:4), pp 504-512.

- van Dyne, L., Cummings, L. L., and Parks, J. M. 1995. "Extra-role behaviors: In pursuit of construct and definitional clarity (a bridge over muddied waters)," in *Research in Organizational Behavior*, L. L. Cummings and B. M. Staw (eds.), JAI Press: Greenwich, CT, pp. 215-285.
- van Dyne, L., Graham, J. W., and Dienesch, R. M. 1994. "ORGANIZATIONAL CITIZENSHIP BEHAVIOR - CONSTRUCT REDEFINITION, MEASUREMENT, AND VALIDATION," *Academy of Management Journal* (37:4) Aug, pp 765-802.
- van Dyne, L., Kamdar, D., and Joireman, J. 2008. "In-role perceptions buffer the negative impact of low LMX on helping and enhance the positive impact of high LMX on voice," *Journal of Applied Psychology* (93:6), pp 1195-1207.
- Williams, K. D., and Sommer, K. 1997. "Social ostracism by coworkers: Does rejection lead to loafing or compensation?," *Personality and Social Psychology Bulletin* (23:7), pp 693-706.
- Williams, L. J., and Anderson, S. E. 1991. "Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors," *Journal of Management* (17:3) Sep, pp 601-617.
- Zhang, X., and Bartol, K. M. 2010. "Linking empowering leadership and employee creativity: The influence of psychological empowerment, intrinsic motivation, and creative process engagement," *Academy of Management Journal* (53:1), pp 107-128.