COMPUTERS & SECURITY 66 (2017) 218–234

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls

*Salvatore Aurigemma* [a,*], *Thomas Mattson* [b]

[a] *University of Tulsa, 800 S. Tucker Dr., Tulsa, OK, 74104, USA*
[b] *University of Richmond, 28 Westhampton Way, Richmond, VA 23173, USA*

ARTICLE INFO

*Article history:*
Received 17 June 2015
Received in revised form 8 February 2017
Accepted 10 February 2017
Available online 16 February 2017

*Keywords:*
Theory of planned behavior
Information security policies
Status
Tailgating
Decomposition of perceived behavioral control
Self-efficacy
Controllability
Hierarchical organizations

ABSTRACT

Existing information security literature does not account for an employee's status (hierarchical relationship (rank order) among employees) within the organizational chain of command when theorizing about his/her information security policy compliance behaviors and behavioral intentions. We argue that this is a potentially important theoretical gap specifically concerning socially interactive threats and controls within hierarchical organizations, because an individual's status within these types of social structures impacts his/her capacity to control another person's resources, behaviors, and outcomes. In this paper, we investigate the main and moderating effect of an employee's status within the organizational hierarchy on an individual's perceived behavioral control related to interactive security threats and controls, specifically tailgating (i.e., the act of gaining access to a restricted area by following someone who has legitimate access). In a survey of Department of Defense employees, we find that the effect of status on perceived behavioral control over tailgating behaviors is positive for employees who report average and above average levels of controllability of coworkers but negative for employees who report below average levels of controllability of coworkers. Our paper has both theoretical and practical value for socially interactive security behaviors within hierarchical organizations with respected levels of command and control.



## 1. Introduction

Threats to an organization's information resources may result from external actors, malicious insiders attempting to defraud the company, or non-malicious insiders who unknowingly and unintentionally put the firm at risk (Warkentin and Willison, 2009). One ubiquitous threat that may involve social interactions among all of these types of actors is tailgating, which is the act of gaining access to a restricted area by piggybacking someone who has legitimate access (Myyry et al., 2009). In a 2014 survey of information security executives, 71% of the respondents indicated that their organizations were vulnerable to a security breach from tailgating (Ritchey, 2015). Physical access controls, including security guards, are effective in partially mitigating the tailgating threat, but these controls do not negate the human threats associated with exhibiting common courtesy (Jensen, 2011). This may be the case because tailgating is as much of a behavioral problem as it is a physical security problem (Greenlees, 2009).

* *Corresponding author.*
*E-mail addresses:* sal-aurigemma@utulsa.edu (S. Aurigemma), tmattson@richmond.edu (T. Mattson).
http://dx.doi.org/10.1016/j.cose.2017.02.006

Interestingly, tailgating requires employees to control their own behaviors in addition to the behaviors of others in order to mitigate the tailgating threat (Jensen, 2011; Peltier, 2006; Ritchey, 2015). Controlling the behaviors of others involves social interactions, which require employees to either verbally or non-verbally communicate with others. It is not possible for an employee to be fully in compliance with typical tailgating information security policies (ISPs) without interfacing with others, because a portion of being in compliance requires observing and enforcing the rules on others, a fact that can be exploited using proven social engineering techniques (Greenlees, 2009; Workman, 2007). The social dynamics of interactions between employees will inevitably vary from company to company due to different organizational structures, cultures, rules, and regulations (Goffee and Scase, 2015; Hofstede and Hofstede, 2005; Schein, 2010). For instance, different types of organizational structures (i.e., traditional hierarchies, flat, flatarchies, holacratic, and networked) may enable or constrain different types of social interactions due, in part, to the presence or absence of respected social hierarchies (Morgan, 2014; Ravlin and Thomas, 2005; Simpson et al., 2012).

Specifically within hierarchical organizations with respected command and control structures, the status (hierarchical relationship (rank order) among employees) of the individuals involved in the interaction may influence the social dynamics of the encounter (Bunderson et al., 2016; Greer and Van Kleef, 2010; Yao and Moskowitz, 2015). For example, in a hierarchical law firm it is probably much easier for a Sr. Partner (high-status employee) relative to a Jr. Associate (low-status employee) to speak up and stop a coworker of any status from tailgating due to the behavioral constraints typically placed on low-status employees. In these types of organizations, an employee's status impacts his/her capacity to control another person's resources, behaviors, and outcomes (Bunderson et al., 2016; Greer and Van Kleef, 2010).

While existing ISP compliance literature has investigated a wide variety of organizational structures (from flat to hierarchical), none of the reported empirical findings accounts for an employee's status when theorizing about an employee's compliance behaviors and behavioral intentions. We argue that this is an important gap in the ISP compliance literature particularly related to socially interactive threats and controls such as tailgating within hierarchical organizations with respected levels of command and control, because status inequalities within these types of organizations impact the dynamics of social interactions (Simpson et al., 2012; Yao and Moskowitz, 2015). The purpose of our paper is to investigate how an employee's status within an organizational hierarchy impacts his/her control over ISP compliance intentions related to socially interactive security threats and controls, specifically tailgating.

In order to do this, we used the theory of planned behavior (TPB) as our theoretical foundation. We used the TPB because this theory has been used extensively in the information security literature but without the inclusion of an employee's status within the organization in any of the traditional TPB paths (Bulgurcu et al., 2010; Dinev and Hu, 2007; Hu et al., 2011; Safa et al., 2015; Siponen et al., 2014; Wynn et al., 2012). Using this theory allows us to determine the incremental impact that status has above and beyond the common factors that have previously been found to impact controllability and compliance intentions. To empirically test the impact of status within the TPB, we surveyed Department of Defense (DoD) employees. Our survey data indicated that an employee's status within the hierarchical DoD had both a direct and moderating impact on his/her perceived behavioral control over compliance behavioral intentions regarding tailgating policies and procedures.

## 2. ISP compliance

Tailgating typically falls under the physical access controls (i.e., controlling the flow of people to authorized areas) section of an organization's ISP (ISO, 2013). There are physical and technical solutions meant to reduce or obviate tailgating, ranging from tailgate sensors to mantraps to biometric devices. However, such technologies can be prohibitively expensive and sometimes physically difficult or impossible to implement properly given physical, legal (owning versus leasing office space), and monetary constraints. For example, the Federal agency responsible for providing adequate information security for all U.S. federal agencies found that physical access control systems deployed in most federal buildings "may offer little or no authentication assurance, because the issued ID cards are easily cloned or counterfeited" (MacGregor et al., 2008). These control system weaknesses have led to compromises of sensitive information resources at private organizations and government facilities (Harwood, 2010) and have resulted in an increased emphasis on employees to prevent unauthorized physical access (Peltier, 2006).

While much of the behavioral ISP compliance literature investigates general ISP compliance across an undefined range of security threats and behaviors, numerous studies explore specific types of security threats (see Table 1). The threats identified in Table 1 are primarily focused on security behaviors

**Table 1 – ISP compliance security threats.**

| Security threat | Related ISP compliance studies |
|---|---|
| Failing to log off work PC | D'Arcy et al. (2014); Johnston et al. (2015) |
| Improper anti-malware software use and maintenance | Workman et al. (2008); Johnston and Warkentin (2010) |
| Improper data storage on USB drive | D'Arcy et al. (2014); Johnston et al. (2015); Guo et al. (2011) |
| Inappropriate system access | D'Arcy et al. (2009); Wynn et al. (2012) |
| Inappropriate data sharing and/or manipulation | D'Arcy et al. (2014); D'Arcy et al. (2009) |
| Installation and use of unauthorized software | Guo et al. (2011); D'Arcy et al. (2009) |
| Poor password management | D'Arcy et al. (2014); Johnston et al. (2015); Guo et al. (2011); Workman et al. (2008) |
| Unsafe and/or inappropriate email practices | D'Arcy et al. (2009); Ng et al. (2009) |
| Use of insecure public wireless networks | Guo et al. (2011) |

that are self-driven where it is largely up to the employee to comply (or not) with the related policy. For example, employee compliance with proper password management policies (i.e., not reusing passwords on multiple accounts, not posting passwords in the open, not sharing passwords, and so on) depends on the individual taking the correct actions per policy requirements beyond that which is automated or enforced by the corporate network. Employee password management requires minimal to no social interaction with colleagues, which means that it is not a reasonable ISP expectation for employees to take responsibility for other people complying with these types of password policies.

Therefore, existing ISP compliance literature does not necessarily make any predictions concerning what would happen to compliance behaviors and intentions regarding security threats and controls that require an employee to interact with a coworker (Furnell and Clarke, 2012; Furnell and Rajendran, 2012). For example, it is difficult to argue that the antecedents to controllability and behavioral intentions related to logging off a work machine would be the same as an employee speaking up and attempting to stop another employee from entering a secure area without the proper credentials. In order to comply with typical tailgating (or physical access) ISPs, employees must control their own behaviors in addition to controlling the behaviors of others (Greenlees, 2009; Ritchey, 2015), which makes the generalizability of the studies displayed in Table 1 to socially interactive threats and controls such as tailgating potentially problematic.

Existing research has relied on a number of theories such as general deterrence theory, protection motivation theory, the TPB along with its predecessor the theory of reasoned action, and rational choice theory in order to explain an employee's ISP compliance intentions (Aurigemma, 2013; Crossler et al., 2013). Similar to the threats investigated in the prior literature, these theories focus on explaining ISP compliance behavioral variability within organizations via self-driven motivators, competencies, attitudes, cost–benefits, and so on. This focus may be appropriate for certain types of threats, but we contend that social interactions with others such as enforcing an ISP on a coworker or a stranger introduces a social dynamic that may be, at least partially, out of an individual's self-control.

Organizations come in many different shapes, structures, and sizes with varying norms and cultures (Goffee and Scase, 2015; Morgan, 2014; Schein, 2010). Certain organizations may develop formal command and control structures that are highly respected by employees whereas other organizations may be flatter with minimal formal reporting structures (Morgan, 2014). Therefore, the types and dynamics of social interactions along with the communication norms may vary somewhat significantly from organization to organization (Bunderson et al., 2016; Ravlin and Thomas, 2005). For instance, in certain hierarchical banks the normative behavior for Jr. analysts may be to not speak up and question executive vice presidents or managing directors, but this may not be the case in other types of banks with different structures, cultures, and norms. Furthermore, not all hierarchical organizations have the same respect for authority (power distance) concerning the command and control structure, which would impact social interaction patterns between employees (Hofstede and Hofstede, 2005; Ravlin and Thomas, 2005; Schein, 2010). It would also not be reasonable to predict that social interactions within, say, a Law firm would be similar to those within a Silicon Valley startup company due to a plethora of contextual differences between those types of organizations. Furthermore, different organizations can develop varying information security cultures (Ruighaver et al., 2007) based upon the management beliefs and characteristics of the organization (Detert et al., 2000).

Yet, the ISP compliance literature has largely not theorized about these organizational differences in terms of their impact on compliance behaviors, particularly those related to socially interactive threats and controls such as tailgating. This stream of literature often assumes, without empirically validating, that there are not any structural enablers or inhibitors to ISP directed behaviors within and/or between organizations (Dhillon et al., 2016; Ramachandran et al., 2013; Ruighaver et al., 2007). One such structural factor that has not been considered is an employee's status in the organizational hierarchy. We propose that this is an important omission particularly in hierarchical organizations with respected levels of command and control, because the employee's status within the hierarchy relative to other employees makes it easier or more difficult to control the behaviors of others (Klein et al., 2006; Sauder et al., 2012; Yao and Moskowitz, 2015).

### 2.1. *Theory of planned behavior (TPB)*

The TPB proposes that individuals are generally rational in terms of their choices and behaviors, which means that their choices and behaviors are governed (at least in part) by their intentions (Ajzen, 1991). More specifically, the TPB predicts that individual choices and behaviors are determined by personal attitudes (state of mind), social pressure from others (subjective norms), and a sense of control (perceived behavioral control) (Ajzen, 1991) (see Fig. 1). The TPB has been extensively used in the behavioral information security literature (Bulgurcu et al., 2010; Dinev and Hu, 2007; Guo et al., 2011; Hu et al., 2011; Ifinedo, 2014; Karahanna et al., 1999; Pahnila et al., 2007; Peace et al., 2003; Siponen et al., 2014; Wynn et al., 2012; Zhang et al., 2009), but without the inclusion of an employee's status within the organization in any of the traditional TPB paths. The status literature, however, strongly suggests that an employee's status particularly within hierarchical organizations with respected command and control structures might impact how much control an individual has over a set of behaviors (Jasso, 2001; Keltner et al., 2003; Yao and Moskowitz, 2015), which is not captured explicitly in any TPB construct.

As with any theory that attempts to model human behavior across a variety of activities, environmental contexts, and conditions, the TPB has limitations leading to reasonable criticisms. For example, the TPB's assertion that humans are generally rational in their behavioral decision-making is frequently criticized as ignoring affective, cognitive, and assorted other biases that impact human judgments and behaviors (McEachan et al., 2011). Ajzen (2011), however, concludes that many of these confounding factors (biases) are antecedents of or are included in the definition of the primary TPB constructs. Furthermore, the TPB is appropriate for our study because it primarily focuses on goal directed behaviors steered by conscious self-regulatory processes. Additionally, the TPB

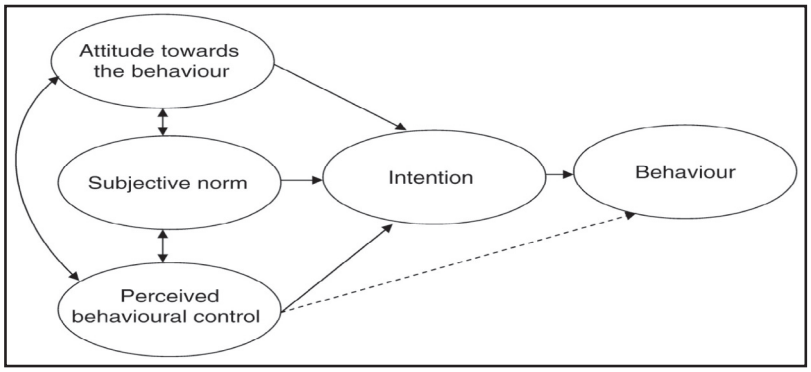


**Fig. 1 – Theory of planned behavior (Ajzen, 1991).**

does not dictate that individual beliefs be free of irrational premises, but that attitudes toward a goal-directed behavior, subjective norms, and perceptions of controllability follow consistently from those beliefs (Ajzen, 2011; Geraerts et al., 2008).

Of the primary TPB constructs evaluated in the ISP compliance literature, the attitude construct has received the most attention. Antecedents for attitudes have been primarily developed using general deterrence theory (D'Arcy et al., 2009; Herath and Rao, 2009a), protection motivation theory (Herath and Rao, 2009b; Johnston and Warkentin, 2010; Ng et al., 2009; Safa et al., 2015; Workman et al., 2008; Wynn et al., 2012), and rational choice theory (Bulgurcu et al., 2010; Workman et al., 2008). Interestingly, research that focuses on the attitude path in the TPB model suggests that there may be certain benefits to non-compliance such as better time management or being able to more efficiently complete job related tasks (Bulgurcu et al., 2010; Workman et al., 2008; Wynn et al., 2012). The benefits from non-compliance are generally included in an individual's attitudes toward compliance or non-compliance intentions within the TPB. Therefore, rational choice theory can be applied to explore the impact of, for instance, the perceived benefits of compliance or non-compliance with tailgating procedures on an employee's attitudes. The focus of our study, however, is not on how an employee's attitudes toward the tailgating phenomena form. Instead, our study focuses on the perceived behavioral control construct within the TPB.

### 2.2. *Perceived behavioral control, self-efficacy, and controllability*

Perceived behavioral control exists to accommodate the potential for any behavior, no matter how common or mundane, to have obstacles impeding a person's perceived ability to perform the behavior (Ajzen, 2002). A person with a higher perceived behavioral control denotes a belief that they have the capability to perform a required action in the face of reasonable obstacles and/or facilitating conditions. In order to more deeply explore the dimensions of perceived behavioral control, we are following the guidance of Taylor and Todd (1995) and Dinev and Hu (2007) by decomposing perceived behavioral control into a multi-dimensional construct. The decomposed perceived behavioral control construct is composed of two components with their own distinctive measures: (1) self-efficacy and (2) perceived controllability.

Self-efficacy is a central tenet of social cognitive theory and represents an employee's belief that he/she is capable of performing a specific behavior, which means higher self-efficacy results in greater effort to persist in the face of obstacles (Bandura, 1997). Whereas self-efficacy represents an individual's perceived ease or difficulty of performing a behavior, perceived controllability addresses beliefs about the extent to which performing the behavior is up to them to carry out (Ajzen, 1991). From an ISP compliance perspective, the distinction between self-efficacy and perceived controllability is clear. For example, an employee's self-efficacy about using strong passwords may be very high because they feel very capable of following guidelines to generate them in their own work setting. Yet, they may exhibit weak control-related beliefs if they are required to ensure that subordinates (for instance) create strong passwords, because they obviously are not directly involved in coworker password creation.

While extensive empirical research indicates self-efficacy and controllability are distinct constructs (Ajzen, 2002), there are clear similarities between the conceptual definitions of self-efficacy and perceived behavioral control. These similarities have led some researchers to use them interchangeably within the ISP behavioral compliance field (Bulgurcu et al., 2010; Herath and Rao, 2009b; Ifinedo, 2012) and in other disciplines (Fishbein and Cappella, 2006; Fishbein and Yzer, 2003; Yi and Hwang, 2003). To justify this substitution, self-efficacy either must account for control-related items in its operational definition, thereby effectively mimicking the definition of perceived behavioral control as a unitary construct or the behavioral context must minimize the need to account for potential control-related obstacles.

One factor that has not been considered as a potential predictor of the deconstructed perceived behavioral control construct is an employee's status within the organization. Particularly within hierarchical organizations with respected levels of command and control, an employee's status (from entry level staffer to CEO) may be a structural impediment or facilitator in terms of how much or how little perceived behavioral control he/she has over a given action (Sauder et al., 2012; Yao and Moskowitz, 2015). An entry-level analyst (low-status employee), for instance, may have high self-efficacy and high perceived controllability but still have low perceived behavioral control over performing an interactive ISP behavior simply due to the entry-level analyst's low position in the organiza-

tional hierarchy. Hierarchical organizations have social inequalities among employees, meaning certain individuals are in more or less advantageous social positions relative to others (DiPrete and Eirich, 2006; Gould, 2002). For instance, in these types of organizations an administrative assistant will logically have less perceived behavioral control over interactive threats and controls relative to a Sr. Vice President. This is the case because an individual's status within a hierarchy provides more or less behavioral constraints (Jasso, 2001; Keltner et al., 2003; Yao and Moskowitz, 2015), which is independent of the employee's self-efficacy and controllability of coworkers.

### 2.3. *Status*

Status is a construct that has broad applicability to a variety of social situations and managerial problems due to the high prevalence of social inequalities across industries and organizations (Bunderson et al., 2016; Magee and Galinsky, 2008; Piazza and Castellucci, 2014). Generally, the literature defines status in one of two ways: (1) a social rank ordering of actors or (2) economic class distinctions between different groups (Berger et al., 1977; Piazza and Castellucci, 2014; Washington and Zajac, 2005). In our paper, we follow the rank order literature (Wejnert, 2002) by defining status as the "prominence of an actor's relative position within a population of actors" (p. 304). In this manner, status refers to a hierarchical relationship among individuals within a particular social setting (Bunderson et al., 2016; Piazza and Castellucci, 2014) whereby those actors in high-status positions are awarded benefits and behavioral liberties not typically available to those actors in low-status positions (DiPrete and Eirich, 2006; Gould, 2002).

Organizational hierarchies may be more prevalent in larger organizations relative to smaller organizations due to the coordination problems associated with managing larger organizations (Goffee and Scase, 2015; Morgan, 2014). Google, for instance, may have started out as a flat (non-hierarchical) organization but as it grew it morphed into a hierarchical organization in order to efficiently and effectively manage its much larger workforce. However, a small organization can also have a distinctive chain of command and hierarchical structure (Lazerson, 1988). For example, a small university of 50 faculty members may certainly have a well-defined rank structure and a respected chain of command. This is also evident in small law firms where a small law firm has clear delineations between and within partnership and associate status levels. Irrespective of the size of the organization, an individual's status within an organizational hierarchy has been found to lead to greater (or less) access to resources, more (or less) organizational power and influence, and an increased (or decreased) capacity to communicate with others (Bunderson et al., 2016; Gould, 2002; Martin, 2009; Sauder et al., 2012).

On the surface it may be logical to conclude that status and self-efficacy or status and controllability will always be highly correlated in the context of information security compliance behaviors associated with interactive threats and controls (i.e., higher status will always lead to greater controllability or greater self-efficacy over ISP directed behaviors). However, this may not be the case. For example, employees typically increase their self-efficacy related to their job tasks when promoted, but job task self-efficacy and information security related self-efficacy are distinct. The newly promoted high-status employee may still have minimal self-confidence in his/her ability to control coworkers related to information security policies, but the new rank may be a structural enabler even without any increased self-efficacy or perceived controllability. Furthermore, a high-status manager who manages staff from all around the world may have increased control over colleagues and subordinates related to job-task deliverables, but may not necessarily have increased control over information security behaviors of colleagues. However, the high-status nature of the position may still impact the manager's overall perceived behavioral control of their security behaviors due to the respected chain of command.

## 3. Research model and hypotheses

Before presenting our proposed research model, we need to note two important boundary conditions. First, we are predicting the impact of status primarily within hierarchical organizations with respected levels of command and control. In these types of organizations employees fully understand to whom they should defer and who should defer to them in the work environment based on formal reporting structures (Bunderson et al., 2016; Simpson et al., 2012). The applicability of our predictions to flatter organizations or to hierarchical organizations with limited respect for the chain of command is not explicitly covered by our research model. Second, we are specifically interested in ISP directed behaviors related to socially interactive threats and controls with a specific emphasis on tailgating. Non-socially interactive ISP directed behaviors are not covered by our research model. Fig. 2 displays our research model.

Having to enforce an ISP requirement on coworkers presents an obstacle that may impact an employee's perceived behavioral control beyond that captured by the self-efficacy construct. For example, typical, physical control policies and procedures require employees to stop other employees who are tailgating and to report those activities to the proper authorities within the organization. This can be a daunting task even for those employees who are high in self-efficacy. Therefore, in this particular context, a decomposed perceived behavioral control construct should be a better indicator of behavioral intent to comply with the ISP relative to self-efficacy alone, because the self-efficacy construct does not capture beliefs about the extent to which performing the behavior is up to them to carry out (Ajzen, 1991).

Conceptualizing perceived behavioral control as a multidimensional construct results in treating self-efficacy as a contributing antecedent to the perceived behavior control construct. In this case, self-efficacy captures the belief of employees in their personal capacity to perform required security actions whereas perceived controllability addresses the beliefs of employees in their ability to overcome control-related obstacles in conducting a security-related behavior. One potential obstacle to comply with most ISPs is having to take action not only on oneself but also on others. If an employee feels as if he/she can generally control his/her coworkers coupled with high self-efficacy, then (given equal conditions) he/she will have

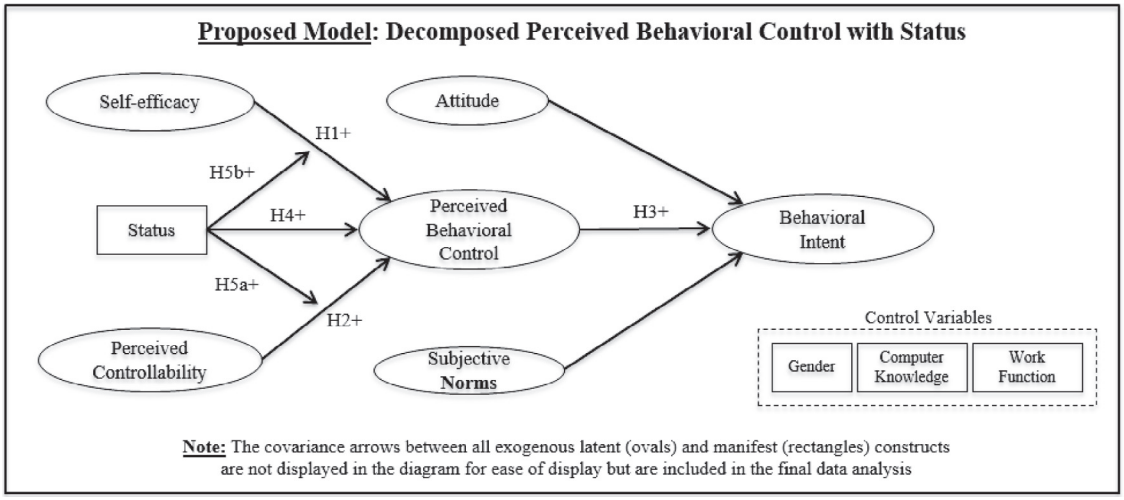


**Fig. 2 – Research model.**

greater perceived behavioral control over socially interactive ISP behaviors. Therefore, we hypothesize the following:

**H1.** *Higher self-efficacy is positively associated with an employee's perceived behavioral control over performing socially interactive ISP behaviors, especially tailgating.*

**H2.** *Higher perceived controllability is positively associated with an employee's perceived behavioral control over performing socially interactive ISP behaviors, especially tailgating.*

**H3.** *Higher perceived behavioral control is positively associated with an employee's intention to follow socially interactive ISP behaviors, especially tailgating.*

However, low-status employees may have a strong belief that they can perform an action (self-efficacy) and have a strong belief that they can generally control their colleagues (perceived controllability), but they may be structurally constrained due to their low-status in the organization. Conversely, a high-status Executive Vice President (EVP) may have low self-efficacy and low perceived controllability over his/her colleagues due to a lack of direct reporting responsibility, but may still have a moderate to high level of perceived behavior control because he/she is in a position of authority within the company. The EVP can modify and influence the behaviors of others simply because he/she holds a high-status position in the company (Sauder et al., 2012; Yao and Moskowitz, 2015). For example, an EVP may be able to prevent tailgating simply by being present when other employees are entering a secure area irrespective of his/her self-efficacy and perceived controllability. An entry level staff member, on the other hand, does not have this structural authority due to his/her low-status (Piazza and Castellucci, 2014; Sauder et al., 2012). Therefore, the status of an employee within an organizational hierarchy impacts his/her perceived behavioral control, because the hierarchy and resulting social positioning of individuals relative to others imposes certain behavioral constraints on the individual (Gould, 2002; Martin, 2009; Sauder et al., 2012), which is independent of their ability to perform an action (self-efficacy) and their belief that they can generally control their colleagues (controllability). As such, we hypothesize the following:

**H4.** *The higher the status of an employee within the organization, the higher the perceived behavioral control over abiding by the firm's socially interactive ISP behaviors, especially tailgating.*

As previously discussed, we expect perceived controllability of coworkers to have a positive effect on perceived behavioral control over socially interactive ISP-directed behaviors. However, we expect the status of the employee to amplify the effect of general controllability of coworkers for high-status employees and cancel the effect of general controllability of coworkers for low-status employees due to the behavioral constraints placed on low-status employees in these types of organizations. We theorize that although low-status employees may feel like they can generally control their coworkers (high perceived controllability), their low-status in the organization ultimately trumps this controllability because low-status employees typically display acts of deference to those in high-status positions in these types of organizations (Klein et al., 2006; Piazza and Castellucci, 2014; Simpson et al., 2012). Furthermore, it is difficult to display acts of deference when pointing out a mistake or a violation to the ISP. This may come across as disrespectful (as opposed to deferential) to the employee in the high-status position. We further predict that status will have much less of an effect on those employees who have a very low belief in their ability to generally control coworkers as we posit that a minimal amount of general controllability over coworkers is required in order to enforce an ISP violation on a colleague. Therefore, we hypothesize the following:

**H5a.** *Effect of controllability on an employee's perceived behavioral control over performing socially interactive ISP behaviors (especially tailgating) is moderated by the status of the employee.*

A key tenet of self-efficacy is the idea that higher self-efficacy leads to more effort to persist in the face of obstacles encountered when performing a particular behavior (Bandura, 1997; Wynn et al., 2012). However, an employee's social status

may hinder this perceived ability to persist, because an individual's status within a social structure impacts his/her capacity to control another person's resources, behaviors, and outcomes (Bunderson et al., 2016; Greer and Van Kleef, 2010; Klein et al., 2006). This means that a low-status employee may have a high degree of confidence in his/her perceived ability to follow the ISP, but his/her low-status unfortunately may cancel out this confidence due to the structural constraints placed on the low-status employee. In certain hierarchical university settings with a respected chain of command, for example, an assistant professor may be very high in self-efficacy but feel that it is inappropriate for a low-status assistant professor to make note of a potential Family Educational Rights and Privacy Act (FERPA) violation by a full professor or to prevent a full professor from tailgating. The structure of typical US universities is such that the full professors (high-status employees) control the resources and the promotion decisions of the assistants (low-status employees), which may qualify the impact of self-efficacy on the perceived behavioral control of socially interactive ISP-directed behaviors. As such, the low-status may trump the effect of self-efficacy in these types of organizations. Therefore, we hypothesize the following:

**H5b.** *Effect of self-efficacy on an employee's perceived behavioral control over performing socially interactive ISP behaviors (especially tailgating) is moderated by the status of the employee.*

## 4. Research design and methods

We collected our data using a survey administered to US DoD employees at multiple organizations, all of whom fell under the same overarching ISP guidance at the time of survey data collection. The DoD is an excellent organization to study employee ISP behavioral compliance intentions because of the presence of a codified set of ISPs, a robust security awareness and training program, and an organizational leadership that values the importance of protecting its expansive information resources. Additionally, the DoD is a hierarchical organization that has a very identifiable and respected status structure both within its military and civilian employees such that employees clearly recognize their status relative to other employees.[1] Numerous DoD information security professionals, senior and middle managers, and employees participated in qualitative discovery and discussions regarding the information security challenges experienced at the individual and organizational level, which further supported the inclusion of status in the research model and the importance of the tailgating threat in this DoD context.

The DoD has very specific requirements for employees to follow in order to protect against the security concerns associated with tailgating. Per the ISP (at the time of the study) and associated training that all participants in this study completed (including successfully passing an assessment on these ISP requirements), DoD personnel are required to perform the following actions in order to combat tailgating: (1) use ONLY (emphasis included) your own security badge or key code; (2) never grant access for someone else; (3) maintain possession of your security badge at all times; (4) challenge people without proper badges; (5) be wary when people with visitor's badges ask about other people's office locations; and (6) report suspicious activity. The above security actions not only direct an employee to not tailgate themselves, but explicitly require that each employee interact with others by observing and challenging others, denying access, and reporting suspicious activity. Therefore, intending to comply with the DoD's tailgating ISPs means an employee intends to comply with all of those elements of the ISP.

After approval by authorized DoD and University Institutional Review Boards, primary data collection was done via an online survey instrument. The participants also had the option to complete the survey in paper form. The survey was designed and administered using best practices outlined by Dillman et al. (2014) such as instruction wording, question order, participant follow-up, and so on. The survey instrument was piloted twice, first with a group of three DoD security management practitioners at different organizations and then with 20 DoD personnel and academics. Each round of reviews focused on question clarity and removing ambiguities, resulting in minor changes to the organization, structure, and content of the survey instrument. A total of 1380 DoD employees were provided the opportunity to participate in the final survey. Per DoD guidelines, individual survey participation was voluntary and responses were anonymous. A total of 317 responses were collected, representing a 23% response rate. After eliminating incomplete surveys, 239 usable surveys were available for analysis.

The measures used to define the latent constructs were adapted from pre-validated (reflective) scales taken from previous ISP-compliance or TPB-related research and we further validated the line items in our pilot studies (see Table 2). All items, except status, were measured reflectively using 7-point Likert scales ranging from (1) strongly disagree to (7) strongly agree. As discussed earlier, we followed the guidance of Taylor and Todd (1995) and Dinev and Hu (2007) by operationalizing perceived behavioral control as a separate construct that mediates the effect of self-efficacy and perceived controllability on behavioral intent. This operationalization of perceived behavioral control not only allows us to better explore the potential impact of status, but it also addresses the statistical concerns with modeling formative constructs in covariance-based structural equation models (CBSEM) (Chin, 1998; Petter et al., 2007), which was the primary analysis technique used in our paper.

[1] We recognize that the DoD is a unique context, but it ideally fits the boundary condition concerning hierarchical organizations with respected levels of command and control. To assess the potential impact of status in other contexts, we conducted informal conversations with employees of varying status levels in different organizations and industries. These informal discussions are not interviews and we did not want to create the impression that we conducted a mixed methods study, so this section of the paper does not mention these informal conversations as part of our method. Instead, we briefly report on the process we followed and the results of these informal conversations in the discussion section of the paper. We received approval from the lead author's institutional review board to conduct these informal discussions, which was a separate IRB process from the main data collection.

**Table 2 – Survey instrument and factor loadings.**

| Variable | Survey question/item | Item | Mean | STD | Back-transformed | | Factor loading | Source(s) |
|---|---|---|---|---|---|---|---|---|
| | | | | | Mean | STD | | |
| Behavioral intent (BINT) | I intend to comply with the tailgating requirements of the ISP of my organization in the future. | BINT1 | 6.657 | 0.484 | 5.687 | 1.472 | 0.866 | Ajzen (1991), Bulgurcu et al. (2010) |
| | I intend to protect information and technology resources according to the tailgating. | BINT2 | 6.661 | 0.483 | 5.707 | 1.453 | 0.944 | |
| | I intend to carry out my tailgating responsibilities prescribed in the ISP of my organization when I use information and technology in the future. | BINT3 | 6.661 | 0.483 | 5.681 | 1.482 | 0.949 | |
| Subjective norms (NORM) | My peers/colleagues think that I should comply with the tailgating requirements of the ISP. | SNFP | 6.414 | 0.722 | 5.502 | 1.565 | 0.902 | Taylor and Todd (1995), Karahanna et al. (1999), Herath and Rao (2009a) |
| | My executives think that I should comply with the tailgating requirements of the ISP. | SNFE | 6.657 | 0.557 | 5.699 | 1.460 | 0.763 | |
| | My subordinates (or those junior to me) think that I should comply with the tailgating requirements of the ISP. | SNFS | 6.293 | 0.829 | 5.367 | 1.619 | 0.843 | |
| Self-efficacy (SEFF) | I have the necessary skills to fulfill the tailgating requirements of the ISP. | SE1 | 6.515 | 0.579 | 5.650 | 1.470 | 0.926 | Bandura (1997), Herath and Rao (2009a), Peace et al. (2003) |
| | I have the necessary knowledge to fulfill the tailgating requirements of the ISP. | SE2 | 6.473 | 0.593 | 5.639 | 1.462 | 0.950 | |
| | I have the necessary competencies to fulfill the tailgating requirements of the ISP. | SE3 | 6.523 | 0.571 | 5.654 | 1.457 | 0.968 | |
| Perceived behavioral control (PBC) | I would be able to follow the ISP for tailgating threats. | PBC1 | 6.381 | 0.693 | 5.629 | 1.482 | 0.845 | Taylor and Todd (1995) |
| | Following the ISP for tailgating threats is entirely within my control. | PBC2 | 6.297 | 0.835 | 5.540 | 1.593 | 0.805 | |
| | I have the resources and knowledge and ability to follow the ISP for tailgating threats. | PBC3 | 6.347 | 0.722 | 5.564 | 1.546 | 0.822 | |
| Attitude (ATT) | Adopting ISP-related security technologies and practices is important for protecting against tailgating threats. | ATT1 | 6.594 | 0.501 | 5.649 | 1.487 | 0.802 | Herath and Rao (2009a), Peace et al. (2003), Riemenschneider et al. (2003) |
| | Adopting ISP-related security technologies and practices is beneficial for protecting against tailgating threats. | ATT2 | 6.607 | 0.506 | 5.642 | 1.491 | 0.914 | |
| | Adopting ISP-related security technologies and practices is helpful for protecting against tailgating threats. | ATT3 | 6.619 | 0.495 | 5.653 | 1.486 | 0.802 | |
| Controllability (CONT) | Enforcing specific guidance and actions directed in the ISP on your coworkers is within your control. | CONT1 | 5.874 | 1.123 | 5.117 | 1.629 | 0.991 | Sparks et al. (1992), Ajzen (2002) |
| | It's mostly up to me to follow the guidance and actions directed in the ISP when I am required to enforce specific ISP policies on my coworkers. | CONT2 | 5.565 | 1.333 | 4.881 | 1.696 | 0.736 | |

Due to excessive skewness and kurtosis of latent variable measurement items, we used log (base 10) transformations for all latent variables, which reduced their skew and kurtosis to acceptable values (Kline, 2011; Ping, 1996). However, we did compare the model results for all of the reported models evaluated in this study using both transformed and non-transformed variable items. The results using non-transformed variable items showed similar effect sizes (given the scale differences), directionality, and significance levels, although model fit while using transformed variables was slightly better, which could be expected after the dataset distribution was normalized by the log (base 10) transformations. Finally, all data were successfully screened for issues that may jeopardize the results, such as outliers, multi-collinearity, and non-normality (Byrne, 2001; Kline, 2011).

Status, the only manifest variable in the model, was represented by a single variable representing military and civilian rank/status on an escalating scale of 1–3 based upon the Geneva Convention and DoD Instruction 1000.01 (change 1, dated June 9, 2014) standards. This resulted in the following ranks: 1 = Non-Commissioned Officer Equivalent (E1-E9 and GS1-GS6), 2 = Company Grade Officer Equivalent (O1-O4 and GS 7–11), and 3 = Field Grade Officer Equivalent (O5 and above and GS 12 and above), where "E" represents enlisted, "O" represents officers, and "GS" represents the general schedule civilian rank.[2] Finally, we mean centered all variables in the perceived behavioral control path (self-efficacy, controllability, and status) in order to facilitate the testing and interpretation of the hypothesized interaction effects, which is consistent with the recommendation of Kline (2011).

To control for potentially confounding factors, we controlled for gender (female/male), general computer knowledge (7-point Likert scale from Very Low to Very High), and primary work function of the respondent (administrative, intelligence, operations, logistics, C4 (command, control, communications, and computers), and command staff element). The gender variable controls for the possibility that it might be easier for males to control the actions of coworkers relative to females regarding socially interactive threats and controls. The general computer knowledge variable accounts for the possibility that employees who are more computer literate (in general) might have greater awareness of general information security threats including tailgating relative to individuals who have minimal computer knowledge, which could increase or decrease ISP compliance intentions across a broad spectrum of threats and controls including (but not limited to) tailgating. The work function variable controls for different contexts. Certain work functions such as intelligence might place greater importance on the tailgating threat than a logistics or event coordinator job function due to the nature of the different jobs. Furthermore, the negative impact of potential data breaches will certainly vary between job functions, so this may differentially impact an employee's compliance intentions.

Two potential sources of biases may exist with our survey: (1) response bias and (2) status-based bias. First, in order to check for possible response and non-response biases, a series of ANOVAs (analyses of variance) were run (1) between groups that finished all sections of the survey and those that did not and (2) between groups that finished the survey before follow-up emails were sent and those that finished the survey after follow-up emails. Results of the ANOVAs showed no statistically significant differences between either sets of groups. Second, in order to ensure that there was not a status-based response bias (i.e., higher ranking survey participants might have a greater or less favorability response bias to report that they intend to follow ISP tailgating requirements) with our anonymous survey, we ran a series of ANOVAs comparing the three different status groups against their reported behavioral intentions to comply with the tailgating threat. Results of the ANOVAs showed no statistically significant differences between rank groupings and reported intention to comply. We also tested for a possible curvilinear relationship between status and the reported behavioral intentions to comply with the tailgating threat, because it is possible that middle-status employees have an increased likelihood of complying due to their unique position in the middle of the organizational hierarchy (Blau, 1960; Dittes and Kelley, 1956; Phillips and Zuckerman, 2001). This squared status term was not a significant predictor of tailgating behavioral intentions in our data.

Due to the nature of the data collection (cross-sectional data during the same time period collected via self-reported questionnaire), common method variance attributed to measurement method instead of the constructs of interest may bias the results (Podsakoff et al., 2003). Several steps were taken to mitigate and assess the potential of common method bias per the guidance in Gefen et al. (2011) and Podsakoff et al. (2003). The survey was administered online (189 responses) and paper-based (50 responses); participation was completely voluntary; respondents were assured anonymity; and the survey stated that there were no right or wrong answers so respondents could answer honestly. We also conducted post-hoc statistical analyses to assess the presence of common method bias. Item level t-test comparisons between online and paper responses indicated no significant differences. We further conducted a Harman's one-factor test and confirmatory factor analysis to test the presence of common method effect. To do this, we entered all model variables into an exploratory factor analysis using principal-component analysis with varimax rotation and unrotated principal-component analysis, both of which revealed four distinct factors with eigenvalues greater than 1.0, and the four factors together accounted for 82.8% of the total variance. The largest factor did not account for the majority of the variance (33.4%). Finally, we performed a confirmatory factor analysis loading all variable items on one factor, because a one-factor confirmatory factor analysis model that does not exhibit common method variance should not fit the data well (Van de Schoot et al., 2012). In our data, the one-factor confirmatory factor analysis model had very bad model fit ($\chi^2$ = 1992.843, df = 119, $\chi^2$/df = 16.747; CFI = 0.562; SRMR = .1658).

[2] We considered deconstructing status into a formative construct containing measures for both formal and informal status, with informal status being calculated using a network measure of centrality (Bunderson, 2003; Bunderson et al., 2016). We did not do this in this paper, because we are interested in *identifiable* status differences related to the command and control structure, which is determined visibly by the formal rank structure in our research context. An informal status metric such as a measure of network centrality may not be readily apparent in a person-to-person tailgating interaction.

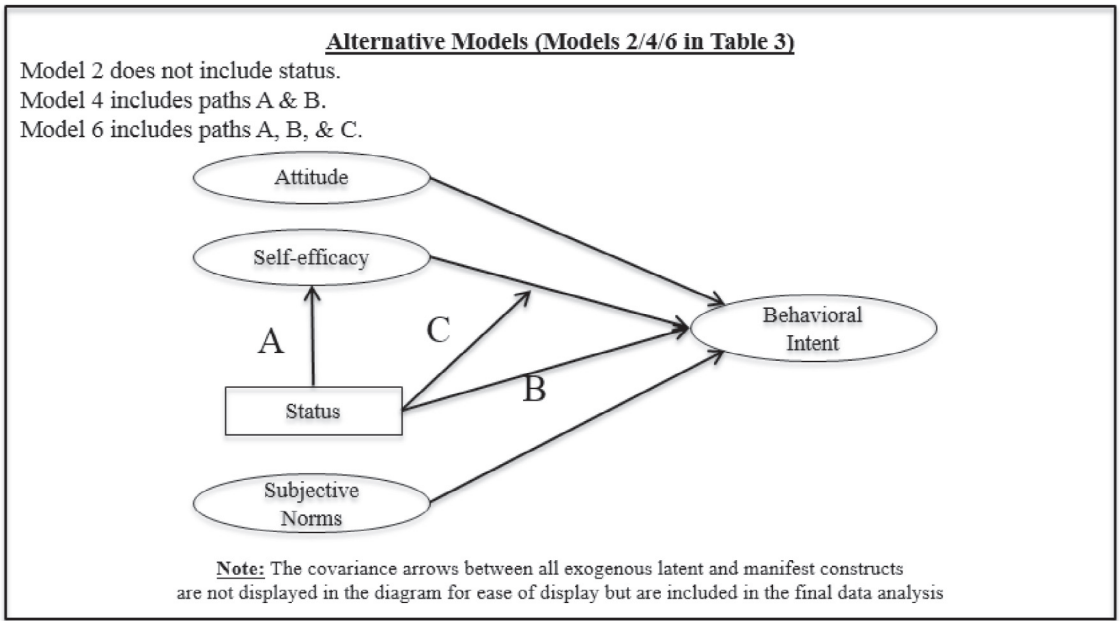


**Fig. 3 – Alternative models.**

While the results of the above analyses do not completely negate the possibility of common method variance, they do suggest that it is not a major concern in these data.

## 5. Results

We tested our research model using covariance-based structural equation modeling (CBSEM) procedures. CBSEM is an appropriate method when testing explanatory relationships between latent constructs of a theoretically derived, *a priori* model (Raykov and Marcoulides, 2006), which is the case for our model. In order to determine whether our hypothesized model was the best fit for our data using CBSEM, we had to compare our proposed (hypothesized) model with several other alternative models. For instance, in order to determine if our data supported the use of the decomposed perceived behavioral control construct, we had to test models using the simpler self-efficacy proxy (used in previous ISP compliance literature) in order to compare model fit and the path coefficients (see Fig. 3 for a complete list of the comparative models).

CBSEM analysis consists of two parts: (1) a confirmatory factor analysis (CFA) stage and (2) the structural model analysis (also known as path analysis) stage (Heck, 1998). The CFA stage assesses the quality and validity of the construct measures and is performed on the entire set of measurement items for all latent constructs simultaneously with each observed variable restricted to load on its a priori factor. Measurement item loadings on their respective constructs are shown in the factor loading column in Table 2 and are all in the range of 0.736–0.99, which are above the recommended threshold of 0.7 (Chin, 1998). To ensure individual item reliability and convergent validity, we examined the average variance extracted (AVE). The AVE values, shown in Table 3, for all latent constructs were greater than the minimum recommended value of 0.50, which indicates that the items satisfied the convergent validity requirements.

We examined the AVE, maximum shared squared variance (MSV), and average shared squared variance (ASV) in order to ensure the discriminant validity of the latent constructs in the research model (see Table 3). In our data, the MSV and ASV were both less than the AVE, which is evidence of discriminant validity because the construct items load more on their respective latent variables than on other constructs (Hair et al., 2010). To confirm the scale reliability and internal consistency of the latent constructs, we calculated composite reliability scores and found them to be greater than 0.7 (Fornell and Larcker, 1981). Based upon the criteria set forth in Jarvis et al. (2003) and Petter et al. (2007), all of the construct measures met the requirements to be considered reflective indicators of their

**Table 3 – Confirmatory factor analysis results.**

| Latent variable | CR | AVE | MSV | ASV | ATT | SEFF | CONT | PBC | BINT | SNORM |
|---|---|---|---|---|---|---|---|---|---|---|
| Attitude (ATT) | 0.876 | 0.702 | 0.563 | 0.181 | 0.838 | | | | | |
| Self-efficacy (SEFF) | 0.964 | 0.899 | 0.543 | 0.253 | 0.351 | 0.948 | | | | |
| Perceived controllability (CONT) | 0.850 | 0.742 | 0.136 | 0.087 | 0.088 | 0.326 | 0.862 | | | |
| Perceived behavioral control (PBC) | 0.864 | 0.679 | 0.543 | 0.248 | 0.304 | 0.737 | 0.369 | 0.824 | | |
| Behavioral intent (BINT) | 0.943 | 0.847 | 0.563 | 0.233 | 0.750 | 0.502 | 0.249 | 0.381 | 0.920 | |
| Subjective norms (SNORM) | 0.878 | 0.707 | 0.324 | 0.190 | 0.342 | 0.492 | 0.353 | 0.569 | 0.377 | 0.841 |

**Table 4 – Structural model results.**

| SEM model fit results | Model 1 | Model 2 | Model 3 | Model 4 | Model 5 | Model 6 | Model 7 | Model 8 |
|---|---|---|---|---|---|---|---|---|
| $\chi^2$/df | 2.523 | 3.379 | 2.466 | 4.773 | 2.254 | 4.327 | 2.407 | 2.212 |
| $\chi^2$ | 257.385 | 162.185 | 281.167 | 276.847 | 281.767 | 289.883 | 303.331 | 302.993 |
| df | 102 | 48 | 114 | 58 | 125 | 67 | 126 | 137 |
| Comparative fit index (CFI) | 0.962 | 0.963 | 0.959 | 0.929 | 0.961 | 0.928 | 0.956 | 0.959 |
| Standardized root mean residual (SRMR) | 0.0594 | 0.0489 | 0.0578 | 0.2262 | 0.0531 | 0.2109 | 0.0554 | 0.0515 |
| Squared multiple correlation (SMC) | 0.725 | 0.645 | 0.723 | 0.611 | 0.724 | 0.611 | 0.723 | 0.725 |
| **SEM structural path results** | | | | | | | | |
| H1: SEFF → PBC | .144*** | | .142*** | | .142*** | | .142*** | .138*** |
| H2: CONT → PBC | .092** | | .093** | | .092** | | .095** | .088** |
| H3: PBC → BINT | .148** | | .134** | | .157** | | .166*** | .156** |
| H4: Status → PBC | | | .011(.097) | | .012* | | .011(.094) | .012* |
| H5a: Status × CONT interaction effect | | | | | .078* | | | 0.081* |
| H5b: Status × SEFF interaction effect | | | | | | NS | NS | NS |
| ATT → BINT | NS | NS | NS | NS | NS | NS | NS | NS |
| SNORM → BINT | .691*** | .644*** | .69*** | .637*** | .694*** | .637*** | .690*** | .692*** |
| (Control) Gender → BINT | NS | NS | NS | NS | NS | NS | NS | NS |
| (Control) Computer knowledge → BINT | NS | NS | NS | NS | NS | NS | NS | NS |
| (Control) Work function → BINT | NS | NS | NS | NS | NS | NS | NS | NS |
| Alternate model: Status → SEFF | | | | NS | | NS | | |
| Alternate model: Status → BINT | | NS | | NS | | NS | | |
| Alternate model: SEFF → BINT | | .151** | | .188*** | | .188*** | | |

Model 1 validates the use of the deconstructed PBC construct. Model 2 tests the main effect of status into BINT while using the SEFF proxy for PBC. Model 3 tests the main effect of status into the deconstructed PBC construct. Model 4 tests whether SEFF as a proxy for PBC might mediate the effect of status into BINT (not PBC). Model 5 tests the STAT by CONT interaction effect using the deconstructed PBC construct. Model 6 tests the STAT by SEFF interaction effect using SEFF as a proxy for PBC. Model 7 tests the STAT by SEFF interaction effect using the deconstructed PBC construct. Model 8 tests both the STAT by CONT and STAT by SEFF interaction effects in the same model using the deconstructed PBC construct.

Note: *p < 0.05, **p < 0.01, ***p < 0.001. SEFF: Self-efficacy, PBC: Perceived Behavioral Control, CONT: Perceived Controllability, BINT: Behavioral Intent, ATT: Attitude, SNORM: Subjective Norms, NS: Not Significant.

respective latent constructs. Finally, the model fit for the CFA analysis was satisfactory ($\chi^2$ = 301.654, df = 104, $\chi^2$/df = 2.901; CFI = 0.951; SRMR = 0.0491).

Following establishment of the measurement model in the CFA stage, we fit the data to the a priori research models and to the alternative (comparison) models (see Table 4). We assessed initial model fit using multiple criteria such as chi-square, degrees of freedom, and normed chi-square ($\chi^2$/df) (Heck, 1998; Kline, 2011; Raykov and Marcoulides, 2006). To further account for the potential impact of even mild deviations from perfectly normal data distributions on the $\chi^2$ calculations, we conducted Bollen and Stine (1992) bootstrapping to calculate model fit p values, which are all above the common 0.05 threshold. However, reliance upon $\chi^2$ measurements alone for model fit determination is cautioned, so we used one goodness-of-fit and one badness-of-fit metric to further assess overall model fit (Kline, 2011).

In our paper, we report the comparative fit index (CFI) as the goodness-of-fit metric. The CFI measures model fit relative to a null model and non-centrality index. All reported CFI values are above the 0.90 (Marsh et al., 2004) or the 0.95 (Hu and Bentler, 1999) recommended thresholds. We further report the standardized root mean square residual (SRMR), which compares the unexplained variance to what would be reasonably expected from a well-fitting model, as the badness-of-fit metric. In all of our theorized research models, the SRMRs are below the common threshold of 0.08, indicating good model fit (Hu and Bentler, 1999).

Table 4 displays the model results for our hypothesized research models (graphically displayed in Fig. 2) and for the alternative models (graphically displayed in Fig. 3). To test our model, we incrementally added constructs to the model in order to evaluate incremental model fit and to compare models representing alternative possible explanations. For instance, a model that had significant path coefficients pertaining to our hypotheses but significantly worse model fit than a more parsimonious model would be weak evidence of our hypotheses. Therefore, we evaluated our proposed research model incrementally in Models 1, 3, 5, 7, and 8. Model 8 represents the full research model with both status interaction effects within the decomposed perceived behavioral control path. We then evaluated alternative models for comparison purposes incrementally in Models 2, 4, and 6. Table 4 provides additional details concerning each model that we report in this paper. None of the control variables were significant for any of the models tested.

The decomposition of perceived behavioral control into self-efficacy (represented by H1) and perceived controllability (represented by H2) are supported in Models 1, 3, 5, 7, and 8. The effect of self-efficacy is highly significant with an unstandardized regression coefficient between 0.138 and 0.144, and the effect of perceived controllability is also highly significant with an unstandardized regression coefficient between 0.088 and 0.095 in all of these models. The decomposed perceived behavioral control latent construct also has a positive and significant relationship (β between 0.134 and 0.166) with behavioral intention to comply with tailgating ISPs in all of these

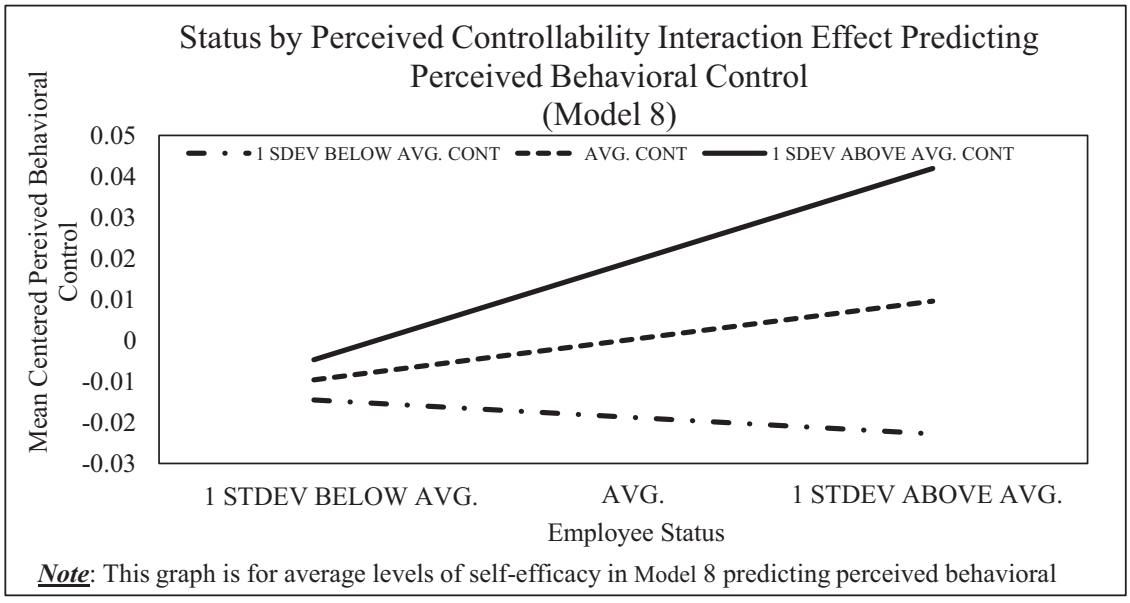


**Fig. 4 – Interaction of status and perceived controllability in model 8.**

models, which supports H3. Rounding out the primary antecedents of behavioral intention to comply with tailgating ISPs in the TPB, subjective norms is a positive and statistically significant contributor (β between 0.637 and 0.694 in Models 1–8) to behavioral intent, but no models revealed a statistically significant effect of attitude on behavioral intention to comply with tailgating ISPs.

The main effect of status (H4) is supported in Models 5 (β = 0.012) and 8 (β = 0.012) at the 0.05 level, but is only significant at the 0.1 level in Models 3 (β = 0.011) and 7 (β = 0.11). This positive effect suggests that while controlling for self-efficacy and perceived controllability, higher-status employees have higher perceived behavior control over following tailgating ISPs. The effect of status is consistent regardless of reported levels of self-efficacy as evident by the not significant interaction effect of status and self-efficacy in Models 7 and 8, which means H5b is not supported. The effect of status, however, is qualified by an employee's perceived controllability of coworkers. In Model 8, for instance, the structural path associated with the interaction effect of status and perceived controllability (H5a) is positive and significant (β = 0.081, $p < 0.05$).

To further interpret the results of the H5a moderation, we plotted the predicted perceived behavioral control for employees of different ranks and different levels of perceived controllability of coworkers (see Fig. 4). As shown in Fig. 4, for employees who report average and above average levels of perceived controllability of coworkers, higher-status employees are expected to have greater levels of perceived behavioral control over the tailgating ISPs. For employees who report below average levels of perceived controllability of coworkers, the effect is reversed (negative slope). In this case, high-status employees are expected to have lower levels of perceived behavioral control relative to low-status employees. Finally, the difference between expected perceived behavioral control over tailgating ISPs is significantly greater for high-status employees relative to low-status employees.

Interestingly, the full alternative model (Model 6) shows no statistically significant impact of status (either a main effect or an interaction effect) when evaluating the TPB with self-efficacy as a proxy for perceived behavioral control. This is in contrast to the reported results in Models 5 and 8 with the decomposed perceived behavioral control hierarchal construct. Therefore, using self-efficacy as a proxy for perceived behavioral control masks the importance of status in the TPB in this study's context (i.e., tailgating ISPs in a hierarchical organization with a well-defined ISP). Additionally, both the hypothesized and alternate models fail to show any significant direct or moderating effect (H5b) between status and self-efficacy. Post-facto ANOVA of reported self-efficacy scores comparing the different status groups validated that there were no significant differences between the groups, which means that higher status employees do not have statistically greater self-efficacy toward tailgating ISPs than lower status employees. This is further evidence that status and self-efficacy are distinct constructs. This post-facto analysis further supports the idea that status's effect on perceived behavioral control is limited to a direct antecedent effect and as a moderator for perceived controllability, but has no significant effect (direct or indirect) on self-efficacy in either the proposed or alternative models.

An implication of our research model is that the decomposed perceived behavioral control construct should have more explanatory power relative to simpler proxies (i.e., self-efficacy alone) in hierarchical organizations with well-defined ISPs in terms of interactive threats and controls such as tailgating. Therefore, in addition to demonstrating statistically significant path coefficients, we examined the model fit statistics associated with our full model (Model 8) and several alternative models (Models 2, 4, and 6). Our full proposed research model (Model 8) is a better fit relative to the full alternative model (Model 6). Model 6 shows weak fit with $\chi^2 = 289.883$ and 67 df, a lower CFI (0.928), and an unsatisfactory SRMR that is well above the acceptable limit (0.211).

Additionally, Model 6's squared multiple correlation (SMC) (CBSEM functional equivalent of $R^2$) of 0.611 shows the alternative model accounts for 61.1% of behavioral intent's variance. In contrast, the full proposed research model (Model 8) shows a markedly better overall model fit ($\chi^2 = 302.993$, 137 df) with a satisfactory CFI (0.959) and SRMR (0.0515). Additionally, the proposed model accounts for 72.5% (SMC = 0.725) of behavioral intent's variance, which is a sizable 11.4% increase over the alternative model. In these data, using self-efficacy as a proxy may not capture an employee's perceived ability to control the actions of coworkers (i.e., speaking up to prevent a fellow employee from tailgating) and doing so may mask the importance of status in the perceived behavioral control path.

## 6. Discussion and conclusions

Our study investigated the main and moderating effect of an employee's status (formal rank) within hierarchical organizations with respected levels of command and control on an individual's perceived behavioral control related to socially interactive security threats and controls (specifically tailgating). In general (on average), we found that high-status employees have greater perceived behavioral control over tailgating ISPs, because they are in a position of authority within organizations (Piazza and Castellucci, 2014; Sauder et al., 2012). In this manner, the position that the employee holds within these types of hierarchical organizations (relative to other employees) has an independent effect on perceived behavioral control over ISP-directed behaviors in conjunction with general controllability of coworkers and self-efficacy.

The significant interaction effect of perceived controllability and status (as shown in Fig. 4) offers at least two theoretically novel insights. First, low-status employees may be deceiving themselves (i.e., overestimating how much control they really have over their colleagues) relative to the structural constraints associated with their low-status position in these types of organizations. Essentially, the employee's low-status appears to minimize the impact of perceived controllability for those employees who report average to above average levels of perceived controllability of coworkers. Second, it is possible that high-status employees have more experience dealing with the managerial aspects of information security violations, which amplifies the impact of perceived controllability for those employees who report average or above average perceived controllability. However, for those high-status employees who already believe that they have less control their coworkers (below average levels of perceived controllability), status may have a negative impact because high-status employees may be less optimistic (relative to their more optimistic low-status colleagues) about being able to positively influence coworker ISP compliance, leading to less perceived behavioral control.

The interaction effect of self-efficacy and status was not significant in any of our models. This means that the impact of self-efficacy on perceived behavior control over the tailgating ISPs was not statistically different for high-, middle-, or low-status employees. This may be the case because tailgating is a threat condition that requires interaction with coworkers (peers, subordinates, and/or superiors). Therefore, status may logically have more of a differential effect on perceived controllability relative to self-efficacy, which is more of an individual construct and less subject to the external constraints associated with an employee's status in the hierarchy in these types of organizations. Nevertheless, future research may investigate the status by self-efficacy interaction effect in other organizational settings and/or with other threat conditions in order to empirically test if self-efficacy has a differential effect for high-, middle-, or low-status employees as we predicted.

Knowing that status differences between employees within these types of hierarchical organizations have a differential effect on perceived behavioral control related to socially interactive threats and controls (specifically tailgating), what can an organization practically do to combat this effect? Information security managers must first determine whether this type of status dynamic is applicable inside of their organizations through observation or by conducting an internal or an external penetration test. As we previously stated, organizations come in many different forms with varying structures, cultures, and norms (Goffee and Scase, 2015; Hofstede and Hofstede, 2005; Schein, 2010) and this status effect may not be readily evident in a particular organizational setting.

If an organization determines that status is adversely impacting compliance intentions related to socially interactive threats and controls, we identify several possible ways to mitigate this effect following the guidance of Luo et al. (2012). Luo et al. (2012) recommend a structured approach to dealing with socially-derived security threats, such as tailgating, which includes updating ISPs and specific procedures related to the security threat of interest, and then propagating these changes through updated security education and training awareness (SETA) programs and materials. First, organizations should conduct separate trainings for high-status members of the organizations. These trainings should explicitly discuss the potential negative impact that their high-status has on their lower status co-workers. In our conversations with high-status DoD personnel, many of them did not recognize that their high-status might adversely impact the behaviors of subordinates or low-status employees. Therefore, having an awareness training specifically targeted for the high-status members of the organization is a good first step toward mitigating the structural effects of status.

Second, after conducting separate trainings for the high-status staff members, we recommend having integrated training sessions with employees across all status levels in order to simulate this status dynamic associated with socially interactive threats and controls such as tailgating. Third, security procedures associated with the ISP should specifically identify techniques for employees of all status levels to use when enforcing anti-tailgating and other socially interactive ISP requirements. One possible technique is having a standardized response or set of socially accepted responses that all employees are encouraged to use for speaking out against potential tailgaters and for addressing employees who are pointing out an information security violation against them. Having these standardized responses may, we speculate, help reduce the adverse social effect of status differences.

Fourth, organizations should consider using security vignettes specifically tailored to the environmental conditions and status distinctions in their organizations to identify

acceptable and unacceptable social responses to socially interactive threats and controls. The use of scenarios and vignettes has been successful in security training and research to address generic security situations and expected behaviors (D'Arcy et al., 2009; Guo et al., 2011; Johnston et al., 2015). We recommended that organizations specifically explore the use of the proposed social engineering attack templates of Mouton et al. (2016) to develop SETA materials directly related to the tailgating threat and the dynamic of relative social status. The templates of Mouton et al. (2016) allow the creation of tailored attack scenarios populated in the context of the specific organization, in this case using access control areas and actual rank/status differences that actually exist in the organization. These scenarios "can then be discussed with the individuals from the organization in a way that enhances the individual's security awareness to be more vigilant" (Mouton et al., 2016, p. 40) against the tailgating threat. Within these training programs, using the standardized responses (from related procedures), simulate and practice social interactions with employees from varying status levels.

Fifth, we recommend considering implementing an anonymous reporting website on the organization's intranet where employees can report on details related to these types of violations (time, location, offender name or description, etc.) without fear of reprisal. The anonymity of the response and using a technical platform removed from the actual event may help lower-status employees feel more comfortable speaking up, with less fear of retribution or retaliation (Gao et al., 2015). Finally, we also suggest posting videos of success stories where a low-status employee successfully prevented a tailgater and integrate those success stories into training sessions. These success stories might help alleviate the perceived behavioral control differences between status groups.

Our study focused on the effect of status on perceived behavioral control (not on subjective norms or attitudes) within the TPB. We made the case that higher status employees (on average) have higher perceived behavioral control over socially interactive threats and controls in these types of organizations relative to their low-status colleagues, because high-status positions are awarded benefits and behavioral liberties not typically available to those actors in low-status positions (DiPrete and Eirich, 2006; Gould, 2002). However, it is also possible that high-status employees develop negative attitudes toward ISP directed behaviors due to their belief that they are above the rules (Appelbaum et al., 2007). For instance, a marketing executive may be giving a tour of the facility to a group of potential clients and she may feel that her tour is more important than any tailgating or physical access control policy, which would decrease her attitude toward compliance. An interesting future study would be to decompose the attitude construct within the TPB using general deterrence theory or rational choice theory in order to investigate the attitudinal differences between high and low status employees within hierarchical organizations with respected command and control structures.

It is important to discuss the potential generalizability of our findings given the DoD context. The primary purpose of our paper is to generalize to theory (Lee and Baskerville, 2003) and our sample provided sufficient variance across all of our variables to test our proposed theoretical relationships within hierarchical organizations containing respected command and control structures. In this manner, the fact that the DoD is an organization that has a wide variety of work functions and a well-defined hierarchy containing both civilian and military employees is a strength of our empirical context. Naturally, however, no descriptive statement (whether quantitative or qualitative) is generalizable beyond the domain that the researcher has actually observed (Lee and Baskerville, 2003), which in our case was the overtly hierarchical DoD. Although we cannot generalize our statistical findings beyond the scope of our DoD sampling frame, we also recognize that there are organizational hierarchies with similar command and control structures in many different industries and organizations. Therefore, we conducted post-hoc informal discussions with employees working in different industries (three bankers/financial services, four hospital workers, six academics, and two attorneys of varying ranks within their organizations) to qualitatively assess the potential impact of status in other industry contexts. We loosely organized these informal discussions around the questions that were on our survey instrument, but did not limit our conversations to just tailgating threats and controls.

Interestingly, our informal discussions revealed that employees in these other industries and organizations identified the importance of knowing one's place in their organizational hierarchies and behaving accordingly as it related to a wide variety of behaviors, including ISP directed behaviors. For example, none of the assistant professors that we spoke to indicated that they would speak out against a full professor or a high-status administrator for any type of information security violation, but only one of the assistant professors knew the specific details of their institution's ISPs and where to locate the actual document on their intranet. This was echoed fairly strongly by the bankers and hospital workers, but less so by the two attorneys we spoke to. We also heard consistently in these informal discussions that lower status employees felt like it was the job of higher status employees to control the ISP behaviors of coworkers. For example, the low-status bankers and attorneys that we spoke to indicated that issues related to controlling coworkers "were above their pay grade," but the middle- to high-status hospital employees indicated that their higher rank required them to focus their efforts on other "more important" issues not related to controlling ISP directed behaviors of other employees (i.e., not my problem). These informal discussions are by no means representative, but they do suggest that status is important in other industry and organizational settings. Therefore, a fruitful area of future research is to investigate empirically the role that status has in other industry contexts, using our theoretical model as a starting point.

Additionally, dissimilar cultures accept status inequalities differently (Triandis, 2000), which means that future research may investigate the potential moderating or mediating role that national culture has on our proposed relationships. For instance, Hofstede's power distance dimension of national culture captures the extent to which a culture accepts status inequalities or, said differently, how much respect a culture has for power and authority (Hofstede and Hofstede, 2005). High power distance cultures such as Russia, India, and China have a high degree of respect for authority and accept status differences as a cultural norm, whereas low power distance cultures such

as Australia, Israel, and Canada have a lower degree of respect for authority and do not accept status differences as a cultural norm (Hofstede and Hofstede, 2005; Triandis, 2000). This suggests the strength of our reported status effects might be stronger or weaker across different national cultures, because the U.S. has a power distance score near the middle (40). An interesting future study might be to conduct a cross-cultural empirical examination of our research model.

It is difficult to manipulate and measure the assorted complexities of specific tailgating encounters using a survey instrument. In our study, we compared and measured general differences across a broad spectrum of tailgating behavioral intentions between employees of different status groups. Our unit of analysis is the average perceived behavioral control per employee based on status differences and not per each potential tailgating incident. For instance, if an employee of any rank attempted to tailgate, would a high-status employee have greater behavioral control of stopping it relative to a middle- or low-status employee (given equal conditions)? An interesting future extension to our work would be to conduct a natural or controlled experiment investigating specific tailgating incidents. This type of study would allow us to investigate the differential effect associated with different sources and different targets using employees at different status levels. For instance, it would be reasonable to surmise that employees at the same low-status level might have similar outcomes as two employees at the same high-status level interacting in a tailgating context. Moreover, status might not even be a factor when two employees of the same status level (irrespective of whether those employees are high-, middle-, or low-status) are interacting in an ISP context, but future controlled experimental research is needed to validate or invalidate this conjecture.

From a methodological standpoint, numerous researchers have pointed out that the use of self-reported survey data is less preferable than evaluating the outcome of actual security behaviors (Anderson and Agarwal, 2010; Crossler et al., 2013; Warkentin et al., 2012). Aptly stated by Crossler et al. (2013), measuring and evaluating self-reported behavioral intentions instead of actual behaviors "is especially troubling because intentions do not always lead to behaviors" (p. 95). These same, and other, researchers are also quick to point out that gaining access to data related to actual security behaviors is a very difficult task, given the extremely sensitive nature of the subject, so some concessions have to be made in order to gain an understanding of such a sensitive phenomenon. In the case of our study, our request to evaluate actual tailgating performance data (field experiments, access control logs, etc.) was denied due to this sensitivity. While we agree that evaluating actual security behavior data would be excellent and extremely valuable, we do not agree that gaining a better understanding (self-reported or not) about user intentions is not valuable. Decades of research on human behavior using theories such as the TPB and protection motivation theory have found that behavioral intent does *generally* lead to actual behavior (Ajzen, 2002; Armitage and Conner, 2001; Floyd et al., 2000). Therefore, it is important to gain a deep understanding of the behavioral antecedents of behavioral intentions, unique insights concerning tailgating threats and controls, and the structural constraints associated with an employee's status, which our paper provides.

## REFERENCES


Ajzen I. The theory of planned behavior. Organ Behav Hum Decis Process 1991;50(2):179–211.

Ajzen I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. J Appl Soc Psychol 2002;32(4):665–83.

Ajzen I. The theory of planned behaviour: reactions and reflections. Psychol Health 2011;26(9):1113–27.

Anderson CL, Agarwal R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q 2010;34(3):613–43.

Appelbaum SH, Iaconi GD, Matousek A. Positive and negative deviant workplace behaviors: causes, impacts, and solutions. Corp Govern 2007;7(5):586–98.

Armitage CJ, Conner M. Efficacy of the theory of planned behaviour: a meta-analytic review. Br J Soc Psychol 2001;40(4):471–99.

Aurigemma S. A composite framework for behavioral compliance with information security policies. J Organ End User Comput 2013;25(3):20.

Bandura A. Self-efficacy: the exercise of control. New York: W.H. Freeman; 1997.

Berger J, Fisek MH, Norman RZ, Zelditch M Jr. Status characteristics and social interaction. New York: Elsevier; 1977.

Blau PM. Patterns of deviation in work groups. Sociometry 1960;23(3):245–61.

Bollen KA, Stine RA. Bootstrapping goodness-of-fit measures in structural equation models. Sociol Methods Res 1992;21(2):205–29.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 2010;34:3.

Bunderson JS. Recognizing and utilizing expertise in work groups: a status characteristics perspective. Adm Sci Q 2003;48(4):557–91.

Bunderson JS, Van Der Vegt GS, Cantimur Y, Rink F. Different views of hierarchy and why they matter: hierarchy as inequality or as cascading influence. Acad Manage J 2016;59(4):1265–89.

Byrne BM. Structural equation modeling with AMOS, EQS, and LISREL: comparative approaches to testing for the factorial validity of a measuring instrument. Int J Test 2001;1(1):55–86.

Chin WW. Commentary: issues and opinion on structural equation modeling. MIS Q 1998;22(1):vii–xvi.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur 2013;32:90–101.

D'Arcy J, Herath T, Shoss M. Understanding employee responses to stressful information security requirements: a coping perspective. JMIS 2014;31(2):285–318.

D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf Syst Res 2009;20(1):79–98.

Detert JR, Schroeder RG, Mauriel JJ. A framework for linking culture and improvement initiatives in organizations. Acad Manage Rev 2000;25(4):850–63.

Dhillon G, Syed R, Pedron C. Interpreting information security culture: an organizational transformation case study. Comput Secur 2016;56:63–9.

Dillman DA, Smyth JD, Christian LM. Internet, phone, mail, and mixed-mode surveys: the tailored design method. Hoboken (NJ): John Wiley & Sons; 2014.

Dinev T, Hu Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J Assoc Inf Sys 2007;8:7.

DiPrete TA, Eirich GM. Cumulative advantage as a mechanism for inequality: a review of theoretical and empirical developments. Annu Rev Sociol 2006;32(1):271–97.
Dittes JE, Kelley HH. Effects of different conditions of acceptance upon conformity to group norms. J Abnorm Soc Psychol 1956;53(1):100–7.
Fishbein M, Cappella JN. The role of theory in developing effective health communications. J Commun 2006;56(s1):S1–17.
Fishbein M, Yzer MC. Using theory to design effective health behavior interventions. Commun Theory 2003;13(2):164–83.
Floyd DL, Prentice-Dunn S, Rogers RW. A meta-analysis of research on protection motivation theory. J Appl Soc Psychol 2000;30(2):407–29.
Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. J Mark Res 1981;18(1):39–50.
Furnell S, Clarke N. Power to the people? The evolving recognition of human aspects of security. Comput Secur 2012;31(8):983–8.
Furnell S, Rajendran A. Understanding the influences on information security behaviour. Comput Fraud Sec 2012;2012(3):12–15.
Gao J, Greenberg R, Wong-On-Wing B. Discussant comment on whistleblowing intentions of lower-level employees: the effect of reporting channel bystanders, and wrongdoer power status. J Bus Ethics 2015;126(1):101–2.
Gefen D, Straub DW, Rigdon EE. An update and extension to SEM guidelines for administrative and social science research. MIS Q 2011;35(2):iii–xiv.
Geraerts E, Bernstein DM, Merckelbach H, Linders C, Raymaekers L, Loftus EF. Lasting false beliefs and their behavioral consequences. Psychol Sci 2008;19(8):749–53.
Goffee R, Scase R. Corporate realities: the dynamics of large and small organizations. New York: Routledge; 2015.
Gould RV. The origins of status hierarchies: a formal theory and empirical test. Am J Sociol 2002;107(5):1143–78.
Greenlees C. Social engineering: an intruder's tale. Eng Technol 2009;4(13).
Greer LL, Van Kleef GA. Equality versus differentiation: the effects of power dispersion on group interaction. J Appl Psychol 2010;95(6):1032–44.
Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding nonmalicious security violations in the workplace: a composite behavior model. J Manag Inf Syst 2011;28(2):203–36.
Hair J, Black W, Babin B, Anderson R. Multivariate data analysis: a global perspective. Upper Saddle River (NJ): Prentice Hall; 2010.
Harwood M. Tailgating leads to thefts inside DC-area business and government offices. In: Security management. Alexandria (VA): ASIS International; 2010.
Heck RH. Factor analysis: exploratory and confirmatory approaches. In: Marcoulides G, editor. Modern methods for business research. Mahwah (NJ): Erlbaum; 1998. p. 177–215.
Herath T, Rao HR. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Dec Supp Syst 2009a;47(2):154–65.
Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst 2009b;18(2):106–25.
Hofstede G, Hofstede GJ. Cultures and organizations: software of the mind. New York: McGraw-Hill; 2005.
Hu L, Bentler PM. Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. Struct Equ Modeling 1999;6(1):1–55.
Hu Q, Xu Z, Dinev T, Ling H. Does deterrence work in reducing information security policy abuse by employees? Commun ACM 2011;54(6):54–60.
Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83–95.
Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf Manag 2014;51(1):69–79.
ISO. ISO/IEC 27002 information technology – security techniques – code of practice for information security management. In: 11. Physical and environmental security. Geneva, Switzerland: International Standards Organization; 2013.
Jarvis CB, MacKenzie SB, Podsakoff PM. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. J Consum Res 2003;30(2):199–218.
Jasso G. Studying status: an integrated framework. Am Sociol Rev 2001;66(1):96–124.
Jensen J. Ready to tailgate? In: Security. 2011. p. 34.
Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Q 2010;34(3):549–66.
Johnston AC, Warkentin M, Siponen M. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q 2015;39(1):113–34.
Karahanna E, Straub DW, Chervany NL. Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. MIS Q 1999;23(2):183–213.
Keltner D, Gruenfeld DH, Anderson C. Power, approach, and inhibition. Psychol Rev 2003;110(2):265–84.
Klein KJ, Ziegert JC, Knight AP, Xiao Y. Dynamic delegation: shared, hierarchical, and deindividualized leadership in extreme action teams. Adm Sci Q 2006;51(4):590–621.
Kline RB. Principles and practice of structural equation modeling. New York (NY): Guilford Press; 2011.
Lazerson MH. Organizational growth of small firms: an outcome of markets and hierarchies. Am Sociol Rev 1988;53(3):330–42.
Lee AS, Baskerville RL. Generalizing generalizability in information systems research. Inf Syst Res 2003;14(3):221–43.
Luo X, Burd S, Li W, Brody RG, Brizzee WB, Cano L. Flying under the radar: social engineering,. Int J Account Inform Manag 2012;20(4):335–47.
MacGregor W, Mehta K, Cooper D, Scarfone K. A recommendation for the use of PIV credentials in physical access control systems (PACS). In: U.S. Department of Commerce, editor. Computer security division, NIST. Gaithersburg (MD): National Institute of Standards and Technology; 2008. p. 71.
Magee JC, Galinsky AD. Social hierarchy: the self-reinforcing nature of power and status. Acad Manag Ann 2008;2(1):351–98.
Marsh HW, Hau K-T, Wen Z. In search of golden rules: comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. Struct Equ Modeling 2004;11(3):320–41.
Martin JL. Social structures. Princeton (NJ): Princeton University Press; 2009.
McEachan RRC, Conner M, Taylor NJ, Lawton RJ. Prospective prediction of health-related behaviours with the theory of planned behaviour: a meta-analysis. Health Psychol Rev 2011;5(2):97–144.
Morgan J. The future of work: attract new talent, build better leaders, and create a competitive organization. Hoboken (NJ): John Wiley & Sons, Inc; 2014.
Mouton F, Leenen L, Venter H. Social engineering attack examples, templates and scenarios. Comput Secur 2016;59:186–209.
Myyry L, Siponen M, Pahnila S, Vartiainen T, Vance A. What levels of moral reasoning and values explain adherence to

information security rules? An empirical study. Eur J Inf Syst 2009;18(2):126–39.
Ng B-Y, Kankanhalli A, Xu YC. Studying users' computer security behavior: a health belief perspective. Dec Supp Syst 2009;46(4):815–25.
Pahnila S, Siponen M, Mahmood A. Employees' behavior towards IS security policy compliance. In: 40th Annual Hawaii International Conference on System Sciences (HICSS 2007). IEEE; 2007. p. 156b.
Peace AG, Galletta DF, Thong JY. Software piracy in the workplace: a model and empirical test. J Manag Inf Syst 2003;20(1):153–78.
Peltier TR. Social engineering: concepts and solutions. Inf Syst Secur 2006;15(5):13–21.
Petter S, Straub D, Rai A. Specifying formative constructs in information systems research. MIS Q 2007;623–56.
Phillips DJ, Zuckerman EW. Middle-status conformity: theoretical restatement and empirical demonstration in two markets. Am J Sociol 2001;107(2):379–429.
Piazza A, Castellucci F. Status in organization and management theory. J Manag 2014;40(1):287–315.
Ping RA Jr. Latent variable interaction and quadratic effect estimation: a two-step technique using structural equation analysis. Psychol Bull 1996;119(1):166–75.
Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology 2003;88(5):879–903.
Ramachandran S, Rao VSC, Goles T, Dhillon G. Variations in information security cultures across professions: a qualitative study. Commun Assoc Inf Syst 2013;33(11):163–204.
Ravlin EC, Thomas DC. Status and stratification processes in organizational life. J Manag 2005;31(6):966–87.
Raykov T, Marcoulides GA. A first course in structural equation modeling. Mahwah (NJ): Lawrence Erlbaum; 2006.
Riemenschneider CK, Harrison DA, Mykytyn Jr. PP. Understanding IT adoption decisions in small business: integrating current theories. Info Manage 2003;40(4):269–85.
Ritchey D. Examining common courtesy. Security 2015;52:1.
Ruighaver AB, Maynard SB, Chang S. Organisational security culture: extending the end-user perspective. Comput Secur 2007;26(1):56–62.
Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. Comput Secur 2015;53:65–78.
Sauder M, Lynn F, Podolny JM. Status: insights from organizational sociology. Annu Rev Sociol 2012;38:267–83.
Schein EH. Organizational culture and leadership. San Francisco: Jossey-Bass; 2010.
Simpson B, Willer R, Ridgeway CL. Status hierarchies and the organization of collective action. Sociol Theory 2012;30(3):149–66.
Siponen M, Mahmood M, Pahnila S. Employees' adherence to information security policies: an exploratory field study. Inf Manag 2014;51(2):217–24.
Sparks P, Hedderley D, Shepherd R. An investigation into the relationship between perceived control, attitude variability and the consumption of two common foods. Europe J Soc Psych 1992;22(1):55–71.
Taylor S, Todd PA. Understanding information technology usage: a test of competing models. Inf Syst Res 1995;6(2):144–76.
Triandis HC. Culture and conflict. Int J Psychol 2000;35(2):145–52.
Van de Schoot R, Lugtig P, Hox J. A checklist for testing measurement invariance. Eur J Dev Psychol 2012;9(4):486–92.
Warkentin M, Willison R. Behavioral and policy issues in information systems security: the insider threat. Eur J Inf Syst 2009;18(2):101–5.
Warkentin M, Straub D, Malimage K. Measuring secure behavior: a research commentary. In: Proceedings of the annual symposium on information assurance. Albany (NY); 2012.
Washington M, Zajac EJ. Status evolution and competition: theory and evidence. Acad Manage J 2005;48(2):282–96.
Wejnert B. Integrating models of diffusion of innovations: a conceptual framework. Annu Rev Sociol 2002;28:297–326.
Workman M. Gaining access with social engineering: an empirical study of the threat. Inf Syst Secur 2007;16(6):315–31.
Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput Human Behav 2008;24(6):2799–816.
Wynn D, Williams C, Karahanna E, Madupalli R. Preventive adoption of information security behaviors. In: Thirty third international conference on information systems. Orlando (FL): 2012 December 16–19.
Yao Q, Moskowitz DS. Trait agreeableness and social status moderate behavioral responsiveness to communal behavior. J Pers 2015;83(2):191–201.
Yi MY, Hwang Y. Predicting the use of web-based information systems: self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model. Int J Hum Comput Stud 2003;59(4):431–49.
Zhang J, Reithel BJ, Li H. Impact of perceived technical protection on security behaviors. Inf Manag Comput Secur 2009;17(4):330–40.

Salvatore (Sal) Aurigemma is an Assistant Professor of Management Information Systems in the Collins College of Business at the University of Tulsa. His research interests are in the behavioral aspects of information security, information privacy, and end-user computing. Prior to joining the University of Tulsa, Sal supported the U.S. Department of Defense for over 20 years on active duty and in the Navy reserves in the submarine and Information Dominance Corps communities. He also has over a decade of civilian experience in the Information Technology field.

Thomas Mattson is an Assistant Professor of Management at the University of Richmond. His research focuses on social interactions in electronic networks of practice, virtual communities of practice, and other electronic social structures along with assorted issues related to information security. Prior to joining academia, Thomas worked as a technology and management consultant designing and building databases and applications for firms in the consumer packaged goods, accounting, and financial industries.