






To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls

Lara Khansa, Jungwon Kuem, Mikko Siponen & Sung S. Kim

To cite this article: Lara Khansa, Jungwon Kuem, Mikko Siponen & Sung S. Kim (2017) To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls, *Journal of Management Information Systems*, 34:1, 141-176, DOI: 10.1080/07421222.2017.1297173



To link to this article: <http://dx.doi.org/10.1080/07421222.2017.1297173>

 View supplementary material 

 Published online: 20 Apr 2017.

 Submit your article to this journal 

 Article views: 64

 View related articles 

 View Crossmark data 

To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls

LARA KHANSA,  JUNGWON KUEM, MIKKO SIPONEN, AND SUNG S. KIM

LARA KHANSA (larak@vt.edu; corresponding author) is an associate professor of business information technology in the Pamplin College of Business at Virginia Tech. She received a Ph.D. in information systems, M.S in Electrical & Computer Engineering, and M.B.A in Finance & Investment Banking from the University of Wisconsin-Madison. Dr. Khansa's research interests include human-computer interaction, online user behavior, online information privacy, and healthcare analytics. Her research has been published in *Journal of Management Information Systems*, *Decision Sciences*, *Communications of the ACM*, *Decision Support Systems*, and other journals.

JUNGWON KUEM (jkuem@wisc.edu) is a Ph.D. student in the Department of Operations and Information Management at the University of Wisconsin School of Business. Her research interests include information security, cyberloafing, smart-phone addiction, and online communities. She holds a Ph.D. in information systems science from the University of Jyväskylä, Finland.

MIKKO SIPONEN (mikko.t.siponen@jyu.fi) is a professor in the Department of Computer Science and Information Systems at the University of Jyväskylä. He holds a Ph.D. in philosophy from the University of Joensuu, Finland, and a Ph.D. in information systems (IS) from the University of Oulu, Finland. His research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. Mikko has published 45 articles in journals such as *MIS Quarterly*, *Journal of the Association for Information Systems*, *Information & Management*, *European Journal of Information Systems*, *Information & Organization*, *Communications of the ACM*, *IEEE Computer*, *IEEE IT Professional*, and others. He has received over €5 million of research funding from corporations and numerous funding bodies.

SUNG S. KIM (skim@bus.wisc.edu) is the Peter T. Allen Professor in the Department of Operations and Information Management at the University of Wisconsin School of Business. He holds a Ph.D. in information technology management from the Georgia Institute of Technology. His research covers issues related to online user behavior including habit, addiction, loyalty, switching costs, information privacy and security, gaming, community participation, and social networking. His work has appeared in *Management Science*, *Information Systems Research*, *Journal of Management Information Systems*, *MIS Quarterly*, *Journal of the Association for Information Systems*, and *Decision Sciences*.

ABSTRACT: We investigate the changing causal relationships between cyberloafing behavior and its antecedents after the announcement of formal organizational controls that, unlike informal controls, are officially imposed by organizations. Drawing on Akers's social learning theory, we first propose neutralization, perceived risk, past cyberloafing, and peer cyberloafing as antecedents of cyberloafing. We then develop a theoretical account of how their impacts change from before to after the announcement of formal controls. The proposed model was empirically tested using data collected from two separate surveys administered a month apart. The first survey captured the preannouncement state of cyberloafing among respondents; the follow-up survey was administered after the respondents were asked to assume that their company had just announced anti-cyberloafing controls that used explicit monitoring and sanctions. We show that preannouncement, employees' intentions to cyberloaf are mostly influenced by their past tendencies to cyberloaf and by others' cyberloafing, but their neutralization and perceived risk play no significant role. In contrast, postannouncement, the impacts of individuals' neutralization and perceived risk on their cyberloafing suddenly become significant. Theoretically, we demonstrate that to accurately predict noncompliant behavior, it is important to account for all four antecedents and incorporate the announcement of formal controls. Practically, understanding how this announcement affects the relationships between cyberloafing and its antecedents suggests different areas managers need to target, pre- and postannouncement, to curb cyberloafing.

KEY WORDS AND PHRASES: cyberloafing, formal controls, neutralization, past cyberloafing, peer cyberloafing, perceived risk, social learning theory.

Cyberloafing, or "nonwork-related computing," refers to employees' surfing the Internet during business hours for personal reasons [14, 48, 49, 61, 79]. Compared with other types of malingering at work (e.g., long lunch breaks, frequent and long personal phone calls, etc.), cyberloafing can potentially have more drastic repercussions on companies' bottom lines because employees can cyberloaf discretely while pretending to be hard at work [1, 48]. Prior research has categorized cyberloafing as a deviant workplace behavior [48, 49], and specifically as a "production deviance" [49, p. 1083] because of its potential to reduce employees' involvement in their work and cause losses in productivity that affect a firm's finances [47, 80]. Importantly, cyberloafing has been shown to increase companies' vulnerabilities and exposure to security risks and to cause overuse of network bandwidth and network disruptions [47, 61]. In addition, the more serious indiscretions that cyberloafers might commit at work, such as online gambling, viewing pornographic movies, or illegally accessing pirated material, can expose companies to potential legal and ethical liabilities (e.g., sexual harassment claims) [61, 79].¹

Over the years, companies have implemented various countermeasures or organizational controls to mitigate the problem of cyberloafing. Controls not officially dictated by the company are generally dubbed informal controls. Such controls could consist of individual ethical beliefs and self-control [18, 37] or social norms [29, 35]—that is, informal signals and cues that give insights into what is or is not socially acceptable by others in the organization, including coworkers and superiors. On the

other hand, formal controls are officially imposed and generally consist of rules and policies, monitoring, and penalties in the event of policy violations [19, 26, 35, 45]. Formal controls have been shown to increase employees' perceptions of accountability [77] and to be more effective at making them follow rules (e.g., [19, 26, 35, 45]). Nevertheless, prior research also found that stringent sanctions and penalties can anger employees and stir perceptions of injustice among them [25, 27, 48, 58, 62, 63]. Consequently, formal controls have the potential to backfire and reinforce employees' intention to cyberloaf as a form of rebellion against the new controls [48, 63]. Despite the anticipated significant influence of formal controls, the current literature offers little insight into whether cyberloafing is driven by the same antecedents before and after the announcement of formal controls. Theoretically, an accurate characterization of cyberloafing behavior requires an understanding of how such an announcement of formal controls affects the relationships between cyberloafing and its antecedents. This essentiality is because before formal controls are announced, one can expect cyberloafing to reflect automaticity in the same way that other types of information technology (IT) use may not reflect deliberate assessment of benefits and risks [41]. Thus, the influence of deliberate and evaluative variables, i.e., neutralization and perceived risk, are likely to be activated only after the formal announcement. On the other hand, the more automatic variables, i.e., past cyberloafing and peer cyberloafing, may be more influential before the formal announcement. Investigating the possibly changing relationships between cyberloafing intention and its antecedents offers significant theoretical value not only to cyberloafing research, but also to social learning theories. From a practical perspective, the lack of focus on how the announcement might affect the nature of the relationship between cyberloafing and its antecedents leaves managers with limited insight into where to direct their efforts to mitigate cyberloafing behavior.

Our objective in this paper is to examine how the announcement of formal controls affects the drivers of cyberloafing. Regardless of the types of controls that might have been in place before, such an announcement generally signals a more serious company stance toward cyberloafing and because of that is expected to affect the characteristics of employee cyberloafing. To achieve this objective, we propose a model of cyberloafing behavior based on Akers' social learning theory (SLT) [3] as our overarching framework. Akers' SLT is one of the first criminology theories to postulate that crime or deviant behavior is dynamically learned [5], rather than being innate and static. As such, it is fundamentally based on the premise that individuals' behavior is integral to their social and environmental contexts. SLT is especially relevant to our study because it proposes antecedents of cyberloafing behavior that are potentially relevant both before and after the announcement of formal controls. Specifically, SLT offers a broader sociopsychological framework in which people's intention to commit deviances is influenced by their tendencies to rationalize or neutralize their deviance (neutralization), their perceptions of the risk of punishments and sanctions (perceived risk), their own past deviant behavior (past cyberloafing), and their coworkers' deviances (peer cyberloafing).

Drawing support from Akers' SLT, we relate neutralization, perceived risk, past cyberloafing, and peer cyberloafing to cyberloafing behavior before and after the

announcement of hypothetical formal organizational controls. We used two surveys administered about a month apart in two different contexts to conduct our analyses before and after the announcement of formal controls. The first survey sought to gauge the existing state of cyberloafing among respondents. The second survey was conducted after respondents were instructed to assume that their company had just announced formal organizational controls to curb cyberloafing. These two experimental stages were separated by the hypothetical announcement of formal organizational controls and thus, respectively, emulate the time periods before and after the actual announcement of organizational controls designed to curb cyberloafing. In the context of this study, the hypothetical organizational controls are formal ones in that they explicitly prohibit employees from cyberloafing and inform them that their Internet activities will be monitored and they will be punished for any violation of the policy. By incorporating a hypothetical announcement of formal organizational controls in a cyberloafing model, we were able to examine the change in the causal relationships between cyberloafing behavior and its antecedents from before to after the announcement.

Our results largely support our proposed theoretical framework. Specifically, both neutralization and perceived risk were found to be significantly related to cyberloafing intention only after the announcement of formal controls. In parallel, other important evaluations, both cognitive (perceived justice) and emotional (anger) that previously were not significantly related to cyberloafing intention suddenly became significant antecedents of cyberloafing intention after their announcement. As stated earlier, our findings carry significant theoretical implications. Particularly, we add to deterrence theory research and its extensions [26], which for the most part advocate formal controls as an effective deterrent of deviant behavior [26] by demonstrating empirically that the announcement of formal controls can actually backfire [25, 27, 62, 63]. This happens by turning factors that previously were not significant determinants of cyberloafing intention (e.g., neutralization, perceived risk, perceived justice, and anger) into significant precursors of cyberloafing intention. In addition to being significant in determining cyberloafing intention after the announcement of formal controls, these factors are also known to have negative repercussions on employees' organizational citizenship behavior, prosocial behavior, and even job satisfaction [25, 58]. Thus, our results imply that the announcement of formal controls could lead to a variety of consequences, which are not necessarily precisely foreseen by managers. Overall, our findings are expected to contribute significantly to the information systems (IS) literature by demonstrating the importance of incorporating the announcement of formal organizational controls in models of cyberloafing behavior, and possibly other noncompliant behavior in organizational contexts, to accurately characterize such behavior.

Theoretical Background

We draw support from Akers's SLT [3] as the basic theory for our model. Traditionally, social learning theories such as SLT help explain the social learning that precedes deviant behavior [3, 4]. SLT fundamentally proposes that the

likelihood that a person will engage in a behavior is affected by the beliefs and attitudes this person holds and by the influences he or she is exposed to [5]. SLT further purports that a person becomes noncompliant when the combined effect of these beliefs, attitudes, and influences in the past, present, and anticipated future favors the violation of law [5, p. 79]. Definitions in SLT stem from people's attitudes and beliefs that affect their behavior [5]. A main category of Akers's definitions corresponds to neutralizing definitions—that is, those that justify the commission of a deviance [5]. SLT is further based on the premise that past experience with a deviance serves as a baseline for future behavior. The mental assessment of the risks of a certain behavior, that is, differential reinforcement, is made relative to that baseline [5]. This differential reinforcement process essentially serves to weigh the pros and cons of noncompliant behavior before deciding whether to proceed. Also of importance in SLT is differential association, which contends that the people a person associates with, such as peers and friends, have a strong influence on the person's behavior. In other words, “you are who you associate with.” SLT has been shown to be useful at studying not only illegal behavior but also legal behavior that violates social rules, such as cyberloafing [48]. Based on Akers's SLT, we propose four variables, namely, neutralization as the facilitator of deviance (definitions), perceived risk as the inhibitor of deviance (differential reinforcement), past behavior as the baseline of deviance, and peer influences (differential association) as the sources of learning for deviance.

Neutralization refers to an employee's attempt to rationalize, excuse, or justify his or her cyberloafing behavior [48]. SLT indicates that definitions, or rationalizations, play a big role in learning deviant behavior. By neutralizing their deviance, employees dampen their sense of guilt and deflect self-disapproval, or others' disapproval of their noncompliant behavior [69]. Several studies have found that employees use neutralization to rationalize their intentions to commit a myriad of deviances, including software piracy [70], information security violations [19, 33, 34, 69], malicious insider attacks (e.g. Internet fraud [46]), and cyberloafing [48, 49]. In the conceptualization of our neutralization construct, we selected the “denial of injury” and “metaphor of the ledger” techniques that have been recognized in the literature as often evoked by cyberloafers [48, 49]. The “metaphor of the ledger” [43] is consistent with the principle of reciprocity in social exchange theory [13] and is often used by cyberloafers who argue that they are entitled to “cash in” on their previously impeccable employee behavior [48, 49]. Similarly, the “denial of injury” technique has been found to be especially espoused by cyberloafers who use it to “downplay” or “trivialize” the consequences of their cyberloafing that, according to them, neither consumes time nor harms the organization [48, 49]. These two neutralization techniques are the most frequently used techniques in the literature in the context of cyberloafing.

Perceived risk, in the context of our study, is a subjective assessment of the undesirable outcomes that employees perceive as associated with cyberloafing. Within the framework of SLT, differential reinforcement implies that deviant behavior would be corrected in the form of punishment. Social learning theorists have

established that the fear of such punishment or probable consequent losses, whether material or reputational, can be used to deter people from continuing their delinquencies [3]. Because cyberloafing could lead to possibly drastic consequences such as job loss and/or humiliation when formal controls are in place, the higher the perceived risk of punishment, the lower the future intention to cyberloaf [49].

Past cyberloafing refers to employees previously engaging in cyberloafing. SLT suggests that a deviant behavior is the result of learning and that it is the reflection of the values and attitudes of an actor toward the behavior. This conjecture is supported by the theory of repeated behavior [41, 64] and its extensions that have been applied in several IS contexts [6, 19, 33, 40, 53]. In a cyberloafing context specifically, and in the absence of formal organizational controls, past cyberloafing has been found to be perpetuated [49, 57, 61, 79].

Peer cyberloafing refers to coworkers' cyberloafing. The concept of differential association within the framework of SLT suggests that individuals are influenced by other individuals or groups with whom they associate. Akers et al. [4] identified peers as the most influential group in defining the reinforcement-punishment contingencies for a similar deviance or alternative behavior. As such, it is expected that noncompliant workplace behavior, such as cyberloafing, will easily spread among employees, especially if cyberloafing has gone unpunished. Prior research has found a strong positive relationship between a worker's antisocial behavior and that of his or her coworkers [3, 4]. A large number of cyberloafing studies reported a significantly positive relationship between peer cyberloafing and cyberloafing behavior [29, 47, 49, 61]. Overall, it has been shown that cyberloafing spreads easily among coworkers and likely will become the norm in the absence of controls to discourage it.

In addition to the four factors based on Akers's SLT, our theoretical framework takes into account other control variables. Specifically, we controlled for perceived justice and anger, which are believed to represent, respectively, cognitive and emotional evaluations of a certain situation in question [23, 59, 65]. Perceived justice refers to employees' perceptions of how fairly their organizations have treated them [65], and anger is the psychological state of distress that one might experience when subjected to situations contrary to his or her will or expectations [59]. Both perceived justice and anger have been found to drive retaliatory and deviant behavior in various settings [25, 27, 35, 48, 58, 62, 63]. In addition, we controlled for self-efficacy, which represents the perception of being focused with clearly set goals [10]. Self-efficacy was found to diminish the effectiveness of anti-cyberloafing organizational controls [61]. Finally, demographically related factors such as age and gender were also taken into account in the conceptual model.

Comparison with Extant Cyberloafing Models

As shown in Table 1, most cyberloafing-related studies have drawn on the theory of planned behavior (TPB) [2] and the theory of interpersonal behavior (TIB) [76] to better characterize cyberloafing behavior and to find effective ways to mitigate it. Some earlier work demonstrated the effectiveness of social factors or subjective

Table 1. Summary of Prior Cyberloafing Literature

Major theoretical frameworks	Cyberloafing literature	Significant antecedents of cyberloafing behavior	
Theory of planned behavior (TPB)	Galletta and Polak [29]; Liberman et al. [47]; Seymour and Nadasen [67]	<ul style="list-style-type: none"> • Attitude • Subjective norms • Perceived behavioral controls 	
Theory of interpersonal behavior (TIB)	Chang and Cheung [17]; Cheung et al. [20]; Moody and Siponen [57]; Pee et al. [61]	<ul style="list-style-type: none"> • Perceived consequences • Social factors • Facilitating conditions • Habit • Affect 	
Akers's social learning theory (SLT)	Our model in this study	<i>Independent variables</i> <ul style="list-style-type: none"> • Peer cyberloafing • Neutralization • Perceived risk • Past behavior 	<i>Control variables</i> <ul style="list-style-type: none"> • Affect (Anger) • Perceived justice • Age, gender; self-efficacy

norms in curbing cyberloafing [29, 47]. For example, using the TPB, Galletta and Polak [29] found that only attitude and subjective norms were effective at curbing cyberloafing. Other work has emphasized the importance of establishing formal controls to effectively curb employees' intention to cyberloaf. For example, Seymour and Nadasen [67], also relying on the TPB, found that only formal controls, were effective at curbing cyberloafing. The ineffectiveness of social norms in their research contradicts that of Galletta and Polak [29], although both studies used TPB. Similarly, Pee et al. [61] and Cheung et al. [20] used the TIB and showed that habit and facilitating conditions were effective at reducing cyberloafing. In contrast, other work [17, 57] found that facilitating conditions did not reduce cyberloafing intention.

None of the work we reviewed has investigated how the announcement of formal organizational controls affects the drivers of cyberloafing behavior. Gaining such insights into the antecedents of cyberloafing behavior before and after the announcement of formal controls is critical to paint a complete picture of cyberloafing behavior and assist managers in designing the right countermeasures. Moreover, ours is the first study to use SLT that alone accounts simultaneously for peer cyberloafing, neutralization, past cyberloafing, and perceived risk.

The research and control variables in our model are not intended to be a comprehensive set of the determinants of cyberloafing behavior. Yet our use of SLT as the overarching theory in the model is believed to be a reasonable representation of

employees' cyberloafing behavior in the workplace. The TPB and TIB are alternative theories that have been used to explain cyberloafing behavior in an organizational context [17, 57, 61]. Originally designed to describe a person's general behavior, these theories indicate that attitude, affect, social norms (social factors), perceived behavioral controls (facilitating conditions), and habit play an important role in regulating human behavior [2, 76]. We argue that in our conceptual model perceived justice and anger—which show the cognitive and emotional factors of special relevance to deviant behavior—correspond, at least to some extent, to the cognitive factor of attitude and the emotional factor of affect [23, 59, 65]. Meanwhile, we expect peer cyberloafing to largely reflect a context-specific dimension of social norms (social factors). Finally, self-efficacy and past cyberloafing in our model closely resemble perceived behavioral controls (facilitating conditions) and habit. The aforementioned discussion suggests that our framework, which is strongly rooted in the SLT, represents a variety of factors relevant to explaining cyberloafing behavior. This inclusion consists of not only those factors already discussed in the TPB and TIB but also other critical factors such as neutralization and perceived risk. Taken together, it is reasonable to argue that our conceptual framework is strongly rooted in a well-established theoretical base and is, at the same time, specific enough to reveal the complex phenomena underlying cyberloafing behavior.

Theory and Hypotheses

Figure 1 shows a conceptual model of the antecedents of cyberloafing behavior before and after the announcement of formal controls. We propose, based on Akers's SLT, that the four antecedents—neutralization, perceived risk, past cyberloafing, and peer cyberloafing—represent the important facets that define an individual as a social learner in society. As noted earlier, our goal was to study how the impact of each of the proposed antecedents on cyberloafing intention changes from before to after the announcement of formal controls. Our model posits that *before the announcement of formal controls, employees' intentions to cyberloaf are mostly influenced by their past tendencies to cyberloaf and by others' cyberloafing*. In contrast, after the announcement of formal controls, *individuals' cyberloafing intentions are also significantly impacted by their neutralization and perceived risk*.

Relationships Between Antecedents of Cyberloafing Intention

In the discussion that follows, we attempt to explain the antecedents of neutralization—that is, past cyberloafing, perceived risk, and peer cyberloafing. We expect these relationships to be significant both before and after the announcement of formal controls.

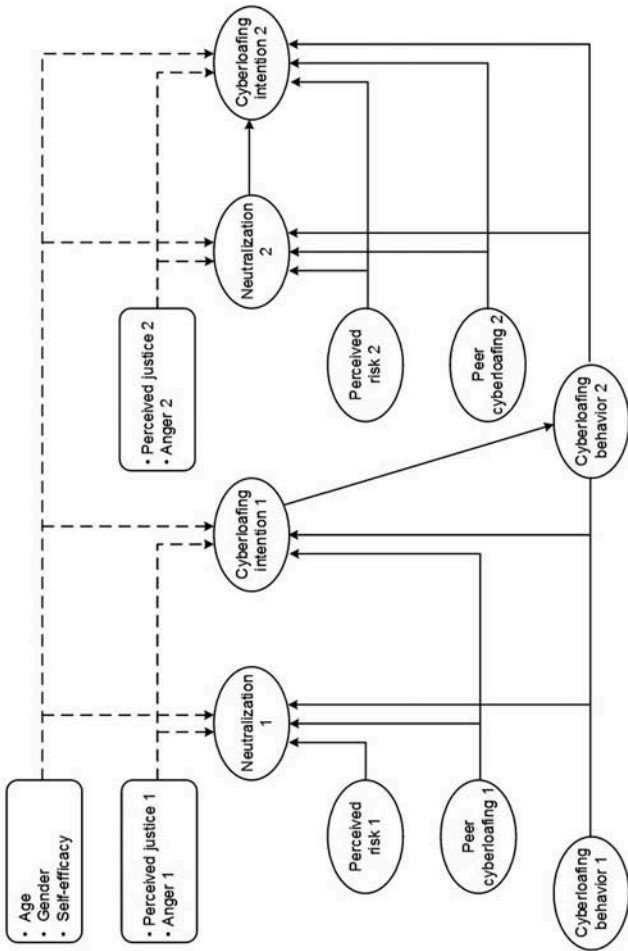


Figure 1. Conceptual Model

Notes:
 Hypothesized relationships are represented with solid lines.
 Relationships involving control variables are represented with dashed lines.

Individuals who have previously engaged in deviant behavior have been shown to perceive a greater need to neutralize their actions as a way to justify their past. For instance, Smith et al. [71] found a significantly positive relationship between prior cheating among business students and their tendencies to evoke neutralization to justify their cheating. Similarly, Koklic et al. [44] found significant evidence that the greater the extent of consumers' past digital piracy, the greater their feelings of guilt and their need to neutralize their past digital piracy. In the context of cyberloafing, employees are likely to evoke neutralization to justify their past cyberloafing that consists of using company resources for personal matters. More specifically, they could also justify their cyberloafing by arguing that despite their past cyberloafing, their performance as employees had met their superiors' expectations or they would have been reprimanded or even fired. Before and after the announcement of formal controls and regardless of their rationale, employees who cyberloafed in the past are likely to be those who see value in it. These employees need to neutralize their cyberloafing as a way to maintain a balance between the benefits they perceive from cyberloafing (e.g., entertainment, relaxation, completing their chores) and what they believe they contribute to their companies in terms of time and productivity.

Hypothesis 1: Past cyberloafing behavior is positively related to neutralization.

Before the announcement of formal controls and regardless of the level of existing controls, employees are likely to fear being stigmatized by their referents and peers for a poor work ethic or for being insufficiently serious and conscientious about their job. Although they might not be reprimanded directly, leaving a bad impression could tarnish their reputation in the longer term and potentially hurt their prospects of promotion or a raise. For these reasons, the higher the perceived risk associated with cyberloafing, the less likely cyberloafers will evoke neutralization to justify it [49]. Given that employees are likely to be rational individuals who strive to keep a positive image of themselves among their peers and superiors at work, the higher the risk they perceive from cyberloafing, the less likely they are to rationalize engaging in it. Thus,

Hypothesis 2: Perceived risk is negatively related to neutralization.

Even before the announcement of formal controls, employees are well aware that cyberloafing is a nonwork activity off-limits to them during regular business hours; thus, they will need to justify such an unproductive behavior. For instance, they could argue that because their coworkers cyberloaf without any official censure, cyberloafing must be acceptable or harmless to the organization. The more pervasive cyberloafing is among their coworkers, the more likely employees will rationalize their engaging in it [48]. For example, employees might argue that cyberloafing must be really beneficial or fulfilling, given that their coworkers cyberloaf despite the formal sanctions against it. They could also neutralize the potential harm to the organization or the seriousness of the formal controls themselves because no harm comes to their peers who cyberloaf with impunity. All in all, we expect that the more

pervasive their peers' cyberloafing, the higher the likelihood employees will rationalize cyberloafing.

Hypothesis 3: Peer cyberloafing is positively related to neutralization.

Antecedents of Cyberloafing Intention

In the following discussion, we attempt to explain the antecedents of cyberloafing intention—past cyberloafing, perceived risk, peer cyberloafing, and neutralization. We expect that these relationships may change between the pre- and postannouncement periods.

In the absence of formal controls prohibiting cyberloafing and explicitly specifying sanctions against violators, cyberloafing is expected to be perpetuated like any other routine activity. In fact, it has been established that in the absence of sanctions, cyberloafing can easily develop into a habitual activity [49, 57, 61, 79]. Thus, the more employees have cyberloafed in the past, the stronger their intention to cyberloaf in the future. However, the announcement of new formal controls prohibiting cyberloafing breaks the routine because it motivates employees to reconsider engaging in their habits and to make a rational choice that would ultimately be in their best interest—one that would benefit them or at least not harm them and their job security. Consequently, although past cyberloafers are more likely to cyberloaf than noncyberloafers, we expect a weakened relationship between past and subsequent cyberloafing after the announcement of formal controls. Thus, we expect that,

Hypothesis 4: Past cyberloafing behavior is positively related to cyberloafing intention before and after the announcement of formal controls, but the relationship is weaker after the announcement.

Before the announcement of formal controls, it can be expected that even if an organization has formal controls in place, users may not be aware of them or, if they are, may pay them little attention because they do not consider them a real or imminent risk [11, 41, 52]. Barnett and Breakwell [11] explain that if people do not consider perceived risk important enough, they are unlikely to change their behavior. In the same vein, before announcement of formal controls, perceived risk ranks too low to affect cyberloafing intention. However, the announcement of formal controls activates perceived risk because it now has the potential to materialize into losses [11]. Because people tend to adjust their behavior when faced with real threats [11], perceived risk becomes a significant deterrent to cyberloafing intention. Taken together, we expect perceived risk to be associated with a reduction in cyberloafing intention only after the announcement of formal controls. Thus,

Hypothesis 5: Perceived risk is negatively related to cyberloafing intention only after the announcement of formal controls but not before.

As discussed previously, pervasiveness of cyberloafing has been shown to result in more cyberloafing [29, 47, 49, 61]. Before the announcement of formal controls, noncyberloafers might feel left out or disadvantaged because their peers' cyberloafing has gone unpunished. If the organization does not make any formal attempt to contain coworkers' cyberloafing, it will likely become the *new norm* and spread organization-wide. The announcement of formal controls marks a turning point because it signals that the organization has become serious about catching and punishing cyberloafers. The newly imposed monitoring and sanctions are likely to reduce the perceived rewards of cyberloafing and are expected to cause a deceleration of the contagion effect among peers but not to eliminate it. On the one hand, employees are tempted to imitate their peers' cyberloafing; on the other, they have a solid indication that punishment is likely imminent if they cyberloaf. In other words, a more rational weighing of the pros and cons of cyberloafing replaces automatic peer imitation. Therefore, the relationship between peer cyberloafing and cyberloafing intention will be significant before and after the announcement of formal controls, but we expect it to weaken when formal controls are in place. Thus:

Hypothesis 6: Peer cyberloafing is positively related to cyberloafing intention before and after the announcement of formal controls, but the relationship is weaker after the announcement.

Applying these same thought processes, before the announcement of formal controls, employees are likely to evoke neutralization retrospectively after they are presented with a hypothetical scenario to ponder. As such, neutralization before announcement of formal controls is a self-perception process [41] that is naturally retrospective and considered neither an important nor necessary determinant of cyberloafing intention. However, after formal controls are announced, neutralization increases in importance in determining intention because justification is needed to challenge the organization's new stance on cyberloafing [5]. For these reasons, we expect that neutralization is significantly related to cyberloafing intention only after the announcement of formal controls.

Hypothesis 7: Neutralization is positively related to cyberloafing intention only after the announcement of formal controls but not before.

Antecedents of Cyberloafing Behavior

The following discussion is devoted to explaining the antecedents of cyberloafing behavior—that is, cyberloafing intention and past cyberloafing.

Triandis [76, p. 203] defined intentions as “instructions that people give to themselves to behave in certain way.” According to the TPB and the TIB, behavioral intentions antecede behavior [2, 76]. Sheeran [68, p. 1] describes this relationship in simple terms: “People do what they intend to do and do not do what they do not intend.” In the specific context of cyberloafing, Bock et al. [14] showed that

intention to cyberloaf is positively related to cyberloafing behavior. We expect a similar relationship between cyberloafing intention and cyberloafing behavior. Thus:

Hypothesis 8: Cyberloafing intention is positively related to subsequent cyberloafing behavior.

Past deviant behavior has been found to be a significant predictor of future deviances [56]. Minor [56] proposed the “hardening process thesis” in which he argues that criminals’ continued deviance erodes their personal norm system, leading to their sustained deviant behavior. This “erosion of morals” [56, p. 1004] weakens cyberloafers’ subsequent moral inhibitions and leads to repeat deviance. Further, from a cost–benefit perspective, as rational individuals, employees who have cyberloafed in the past have reaped benefits from it [49, 57, 61, 79]. Although formal controls might increase the expected costs of cyberloafing, they do not eliminate its perceived benefits. This is especially true given that the aforementioned cyberloafers were not punished for their cyberloafing; therefore, the perceived costs of cyberloafing were never actually realized. All in all, we expect a positive relationship between past cyberloafing and subsequent cyberloafing.

Hypothesis 9: Past cyberloafing behavior is positively related to subsequent cyberloafing behavior.

Method

Data Collection

We performed a two-wave study to closely monitor any changes in individuals’ perceptions and behavior toward cyberloafing subsequent to the announcement of formal organizational controls. In this two-wave study, we first conducted a survey of the current, presumably ordinary, state of cyberloafing among respondents. About four weeks later, we performed a follow-up survey in which the respondents were instructed to assume that their company had announced formal controls to curb cyberloafing and then to answer questions about how they would react to such an announcement. In summary, to study the varying dynamics of individuals’ cyberloafing over time, we conducted two separate surveys, one before the announcement of hypothetical organizational controls and the other afterward.

To collect data, we worked with a market research firm that manages a nationwide online panel. A sample frame was drawn from panel members who at the time of the survey had a full-time or part-time job working at an organization with five or more employees. Potential subjects were asked to take an online survey in return for a small dollar amount deposited in their PayPal accounts. We initially recruited 62 subjects for a pilot test of an early version of our questionnaire. Based on the results of the pilot test, we clarified the instructions and questions in the survey to improve the readability and psychometric properties of our measurement instrument. Specifically, to avoid any confusion that might arise about the actual meaning of

cyberloafing, we explicitly defined cyberloafing at the beginning of the survey instructions as *Internet use at work for personal purposes*.

After the pilot test, we performed a main study that consisted of two different surveys administered about four weeks apart. In Survey 1, we chose 2,000 U.S.-based members from the panel pool and sent them e-mail invitations to participate in our survey. Each invitation included a link to a web-based questionnaire and a statement that all personal information would be kept strictly confidential. In this survey, a total of 451 responses were collected, which represents a response rate of 22.6 percent. The average age of respondents was 44, and 54 percent of the respondents were male. To check for nonresponse bias, we compared the demographic profiles of respondents and nonrespondents, but we did not find any significant differences in terms of age and gender ($ps = ns$).

Four weeks later, we sent invitations to participate in Survey 2 to all 451 respondents who had completed the first survey. We also sent each respondent an e-mail invitation that included a link to a web-based questionnaire. This follow-up invitation received 360 completed surveys, representing a response rate of 80 percent. The average age of these 360 respondents was 45, and 55 percent were male. We checked for the possibility of nonresponse bias by comparing those who responded only to the first survey and those who responded to both surveys. No significant differences were found between the two groups in terms of age and gender ($ps = ns$). We found that 80 percent of the respondents were employed full-time, 45 percent worked at large companies with 500 or more employees, and 56 percent ranked as middle- or upper-level employees (55.6 percent). For our subsequent data analysis, we used the 360 responses collected from those who responded to both surveys.

Measures

Appendix A displays the specific items and scenarios used in this study. Survey 1 and Survey 2 were almost identical in that they measured essentially the same factors: cyberloafing, perceived risk, peer cyberloafing, neutralization, cyberloafing intention, self-efficacy, perceived justice, and anger. The only differences between them were that whereas Survey 1 included personal characteristics such as age, gender, and general self-efficacy, Survey 2 contained a hypothetical scenario. The scenario involved an e-mail notification of an organizational policy on cyberloafing. In this scenario, a company informed its employees that cyberloafing would result in disciplinary actions up to and including termination.² In Survey 2, all subjects were asked to respond to survey items by assuming that the situation described in the scenario applied to them.

Most of the measurement items in this study were adapted from previous research. In those instances in which appropriate measures were not available in the literature, we carefully developed new items. First of all, cyberloafing behavior was measured with two items adapted from the two-item scale of behavioral frequency in [50]. Perceived risk was measured with three items modified from the scale of formal

sanctions in Siponen and Vance [69]. We adapted the scale of descriptive norm from Anderson and Agarwal [7] to create a two-item scale of peer cyberloafing. Neutralization was measured with three items adapted from Siponen and Vance [69]. Three items were adapted from Venkatesh and Davis [78] to measure cyberloafing intention. The scale of self-efficacy included three items adapted from Taylor and Todd [75]. To measure justice, we used three items that were modified from the scale of global fairness in Schmidt et al. [65]. Finally, the scale of anger, which included three items, was borrowed from Nyer [59].

Results

Measurement Model

To assess our measurement model, we performed a confirmatory factor analysis (CFA) using LISREL 8 [39]. Five fit indices were used to evaluate the model [21, 30, 42]. The indices used in this were the comparative fit index (CFI), the non-normed fit index (NNFI), the root mean square error of approximation (RMSEA), and the standardized root mean square residual (SRMR), the goodness-of-fit index (GFI), and the adjusted goodness of fit (AGFI). A model is considered acceptable if $CFI \geq 0.95$, $NNFI \geq 0.95$, $RMSEA \leq 0.06$, $SRMR \leq 0.08$, and $AGFI \geq 0.80$ [12, 30, 36]. Our model consisted of 15 factors with 45 items, which included two one-item scales of age and gender. The results of CFA showed that the measurement model was highly satisfactory: $\chi^2(811) = 1,410.45$, $p < 0.001$, $CFI = 0.98$, $NNFI = 0.98$, $RMSEA = 0.043$, $SRMR = 0.045$, $AGFI = 0.81$. Table 2 shows the means, standard deviations, composite reliability (CR), average variance extracted (AVE), and correlations of the measures based on the results of the measurement model.

After assessing the overall fit of the model, we examined the psychometric properties of the scales in this study in terms of reliability, convergent validity, and discriminant validity. We used CR and AVE to evaluate the reliability of the scales [9, 28]. The reliability of a scale is considered adequate if CR and AVE values exceed 0.7 and 0.5 [9, 28]. As shown in Table 2, the CR and AVE values exceeded the recommended cutoff values of 0.70 and 0.50, respectively (i.e., $CRs \geq 0.83$ and $AVEs \geq 0.71$) [9, 28]. Subsequently, we assessed the convergent validity of the scales by comparing the item loadings with the recommended minimum value of 0.60 [21]. We found from the results of the measurement model that the lowest item loading was 0.65, which demonstrates adequate convergent validity. Finally, discriminant validity was examined by comparing the original measurement model with a constrained model in which a correlation between two factors is set to unity [8, 9]. Specifically, each pair of factors was modeled in two different confirmatory factor models: One allowed the pair to freely correlate; the other restricted the correlation to unity. A series of chi-square difference tests were performed to formally check whether the correlation of any pair is statistically not different from one. The results of the tests revealed that no pair differed from unity, which shows a satisfactory level of discriminant validity [66].

Table 2. Properties of Measurement Scales

	ME	SD	CR	AVE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
1. AGE	44.7	11.1	na	na	1.00																	
2. GEN	1.5	0.5	na	na	0.24*	1.00																
3. SE	5.9	1.2	0.94	0.83	-0.17*	-0.05	1.00															
4. PUJ	5.1	1.3	0.94	0.83	-0.03	-0.08	0.32*	1.00														
5. ANG1	2.9	1.6	0.93	0.81	-0.04	-0.05	-0.24*	-0.26*	1.00													
6. CB1	3.3	1.9	0.84	0.72	-0.29*	-0.24*	0.20*	0.28*	-0.10	1.00												
7. PR1	3.9	1.8	0.94	0.79	0.03	0.00	-0.18*	-0.17*	0.44*	-0.36*	1.00											
8. PC1	5.6	1.3	0.83	0.71	-0.03	-0.14*	0.48*	0.42*	-0.24*	0.45*	-0.34*	1.00										
9. NEU1	4.4	1.9	0.94	0.83	-0.24*	-0.16*	0.29*	0.30*	-0.21*	0.66*	-0.48*	0.59*	1.00									
10. CI1	4.7	2.3	0.98	0.93	-0.24	-0.14*	0.23*	0.26*	-0.08	0.80	-0.35*	0.49*	0.61*	1.00								
11. PJ2	5.1	1.4	0.93	0.81	0.05	0.03	0.12*	0.32*	0.06	-0.04	0.17*	0.02	-0.05	-0.03	1.00							
12. ANG2	3.3	1.7	0.92	0.80	-0.28*	-0.16*	0.06	-0.02	0.11*	0.40*	-0.08*	0.19*	0.37*	0.33*	-0.33*	1.00						
13. CB2	3.6	1.9	0.86	0.75	-0.28*	-0.15*	0.11	0.18*	-0.08	0.86*	-0.27*	0.38*	0.55*	0.76*	-0.04	0.37*	1.00					
14. PR2	4.5	1.7	0.92	0.75	0.01	0.02	0.11*	0.07	0.10*	-0.17	0.34*	0.10	-0.13*	-0.15*	-0.03	0.18*	-0.19*	1.00				
15. PC2	5.3	1.3	0.87	0.77	0.12*	-0.05	0.20*	0.21*	-0.05	0.18*	-0.04	0.51*	0.26*	0.25*	0.15*	0.02	0.19*	-0.17*	1.00			
16. NEU2	4.4	1.8	0.95	0.87	-0.18*	-0.17*	0.11	0.15*	-0.09	0.52*	-0.31*	0.39*	0.60*	0.46*	-0.10	0.31*	0.52*	-0.33*	0.50*	1.00		
17. CI2	3.8	2.2	0.97	0.92	-0.25*	-0.19*	0.15*	0.14*	-0.02	0.62*	-0.20*	0.28*	0.47*	0.59*	0.03	0.27*	0.69*	-0.46*	0.36*	0.64*	1.00	

* $p < 0.05$ (two-tailed test).

Notes: ME = mean; SD = standard deviation; CR = composite reliability; AVE = average variance extracted. AGE = age, GEN = gender, SE = self-efficacy, PUJ = perceived justice at $t = 1$; ANG1 = anger at $t = 1$; CB1 = cyberloafing behavior at $t = 1$; PR1 = perceived risk at $t = 1$; PC1 = peer cyberloafing at $t = 1$; NEU1 = neutralization at $t = 1$; CI1 = cyberloafing intention at $t = 1$; PJ2 = perceived justice at $t = 2$; ANG2 = anger at $t = 2$; CB2 = cyberloafing behavior at $t = 2$; PR2 = perceived risk at $t = 2$; PC2 = peer cyberloafing at $t = 2$; NEU2 = neutralization at $t = 2$; CI2 = cyberloafing intention at $t = 2$.

We attempted to assess the extent of common-method variance (CMV) by using the marker-variable technique [51, 55]. As done in prior IS research, fantasizing was used as a marker variable [55, 72]. Fantasizing, which refers to the extent to which a person has a vivid imagination, was measured with three items adapted from O’Guinn and Faber [60]. Lindell and Whitney [51] have suggested that the smallest correlation between the marker variable and other research variables is a reasonably conservative estimate of CMV. Accordingly, we added fantasizing into the earlier measurement model and then tested the revised measurement model. Although not reported in this study for the sake of brevity, the results showed that the smallest correlation between the marker variable and research variables was essentially negligible ($r = 0.01$, $p = \text{ns}$). Overall, the results of the marker-variable analysis suggest that CMV, if any is present, is not a significant factor in our study.

Proposed Model

To test our proposed model, we used a structural equation modeling (SEM) tool, LISREL 8 [39]. Figure 2 depicts the results of the proposed model with significant relationships. In the case of this model, the fit indices were well within the satisfactory ranges [$\chi^2(845) = 1,515.94$, $p < 0.001$, CFI = 0.98, NNFI = 0.98, RMSEA = 0.047, SRMR = 0.046, AGFI = 0.81]. This model explained on average about two-thirds (i.e., 65 percent) of the variation in research variables. Interestingly, after controlling for peer cyberloafing and past cyberloafing, neutralization at $t = 1$ became trivial in determining cyberloafing intention at $t = 1$ (estimate = 0.03, $p = \text{ns}$), although neutralization at $t = 2$ was still a significant antecedent of cyberloafing intention at $t = 2$ (estimate = 0.21, $p < 0.001$). Similarly, perceived risk was a significant predictor of cyberloafing intention only at $t = 2$ (estimate = -0.32 , $p < 0.001$), but not at $t = 1$ (estimate = -0.06 , $p = \text{ns}$). In general, our results suggest that the proposed model is a reasonable representation of reality and could serve as a solid basis for understanding individuals’ changes in cyberloafing behavior over time in reaction to the announcement of formal organizational controls.

As is evident in Figure 2, perceived risk, peer cyberloafing, and cyberloafing behavior had significant impacts on neutralization and cyberloafing intention with one exception. This exception was the relationship between perceived risk and cyberloafing intention. Meanwhile, the control variables do not seem important in regulating neutralization and cyberloafing intention. Specifically, age, gender, and self-efficacy did not have any significant impact—with one exception—on neutralization or cyberloafing intention. The exception was found in the negative relationship between age and neutralization at $t = 1$, which implies that people tend to rationalize their behavior less as they age (estimate = -0.10 , $p < 0.05$). Similarly, perceived justice and anger did not have any significant influence on either neutralization or cyberloafing intention before the announcement of organizational controls. However, they were significant factors for neutralization and cyberloafing intention after the announcement. Specifically, we found that neutralization

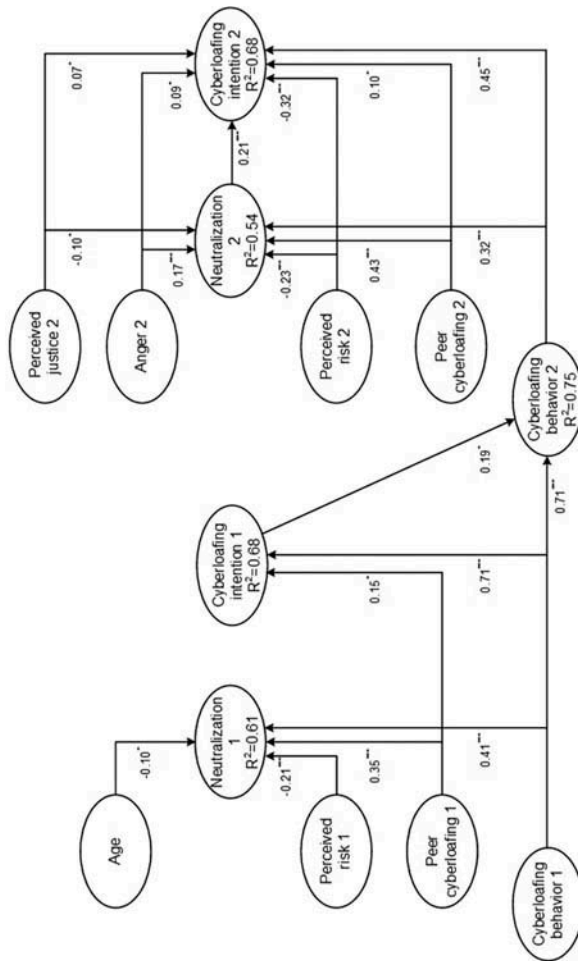


Figure 2. Results of the Proposed Model

Notes:

n = 360.

Only significant paths are shown.

* p < 0.05, ** p < 0.01; *** p < 0.001.

decreased as perceived justice increased (estimate = -0.10 , $p < 0.05$), but cyberloafing intention increased with the increase in perceived justice (estimate = 0.07 , $p < 0.05$). Moreover, anger was positively associated with neutralization (estimate = 0.17 , $p < 0.001$) as well as with cyberloafing intention (estimate = 0.09 , $p < 0.05$). Overall, our findings indicate that research variables largely explained neutralization and cyberloafing intention, but perceived justice and anger were also important factors affecting neutralization and cyberloafing intention, especially after the announcement of formal organizational controls.^{3,4}

Tests of Research Hypotheses

In general, our data strongly supported our hypotheses. Of the nine hypotheses we proposed, eight were fully supported. The ninth was partially supported. Table 3 summarizes the research hypotheses and their results. The specific results of the hypotheses are described as follows:

Neutralization. We earlier predicted that neutralization is a function of cyberloafing behavior, perceived risk, and peer cyberloafing before and after the announcement of formal organizational controls. As shown in Figure 2, past cyberloafing is a significant antecedent of neutralization at $t = 1$ (estimate = 0.41 , $p < 0.001$) and at $t = 2$ (estimate = 0.32 , $p < 0.001$) (H1 supported). Similarly, we found that perceived risk was significant in determining neutralization before (estimate = -0.21 , $p < 0.001$) and after the announcement of formal controls (estimate = -0.23 , $p < 0.001$) (H2 supported). In addition, peer cyberloafing was found to significantly influence neutralization at $t = 1$ (estimate = 0.35 , $p < 0.001$) and at $t = 2$ (estimate = 0.43 , $p < 0.001$) (H3 supported).

Cyberloafing intention. Unlike the formation of neutralization, cyberloafing intention was hypothesized as subject to more complex processes. First, we hypothesized that the effect of past behavior on intention would be significant at all times, but its relationships would be stronger at $t = 1$ than that at $t = 2$. As Figure 2 indicates, the relationship at $t = 1$ (estimate = 0.71 , $p < 0.001$) appears to be considerably stronger than that at $t = 2$ (estimate = 0.45 , $p < 0.001$), although both relationships are statistically significant. To formally test the hypothesis, we performed a chi-square difference test. In this test, an unconstrained model (i.e., the proposed model) was compared with a constrained model in which the two estimates were specified to be equal. The result showed that the strengths of the two relationships were not equal but actually significantly different, supporting our hypothesis [$\Delta\chi^2(1) = 508.14$, $p < 0.001$] (H4 supported). Second, we suggested that perceived risk would be an important antecedent of intention only after formal controls. Consistent with this prediction, the effect of perceived risk on cyberloafing intention was found not to be significant at $t = 1$ (estimate = -0.06 , $p = \text{ns}$) but significant at $t = 2$ (estimate = -0.32 , $p < 0.001$) (H5 supported). Third, our hypothesis states that peer cyberloafing would be a significant factor in cyberloafing intention at all times, but its relationship would be stronger at $t = 1$ than that at $t = 2$. We found that the effect of peer

Table 3. Results of Research Hypotheses

Hypothesis	Prediction	Path estimates			Hypothesis test
		Before the announcement of formal controls	After the announcement of formal controls		
H1: CB → NEU	Positive and equal in both conditions	0.41***	0.32***		Supported; positive in both conditions
H2: PR → NEU	Negative and equal in both conditions	-0.21***	-0.23***		Supported; negative in both conditions
H3: PC → NEU	Positive and equal in both conditions	0.35***	0.43***		Supported; positive in both conditions
H4: CB → CI	Positive in both conditions, weaker effect under formal	0.71***	0.45***		Supported; positive in both conditions; $\Delta\chi^2$ significant
H5: PR → CI	Negative only under formal	ns	-0.32***		Supported; negative only under formal
H6: PC → CI	Positive in both conditions, weaker effect under formal	0.15*	0.10*		Partially supported; positive in both conditions; $\Delta\chi^2$ not significant
H7: NEU → CI	Positive only under formal	ns	0.21***		Supported; positive only under formal
H8: CI → CB	Positive		0.19*		Supported; positive
H9: CB → CB	Positive		0.71***		Supported; positive

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$ (two-tailed test).

Notes: CB= cyberloafing behavior; PR = perceived risk; PC = peer cyberloafing; NEU = neutralization; CI = cyberloafing intention.

cyberloafing on intention was indeed significant at $t = 1$ and at $t = 2$, and the relationship at $t = 1$ (estimate = 0.15, $p < 0.05$) seemed to be stronger than the relationship at $t = 2$ (estimate = 0.10, $p < 0.05$). We performed a chi-square difference test again to check if the difference in relationship strengths was significant. However, the result indicated that contrary to our expectation, the two relationships were not significantly different [$\Delta\chi^4(1) = 1.32, p = \text{ns}$]. These results as a whole only partially support our hypothesis on the effect of peer cyberloafing on cyberloafing intention (H6 partially supported). Finally, we predicted that the effect of neutralization on intention would be significant at $t = 2$ but not at $t = 1$. As expected, neutralization did not have a significant effect on intention at $t = 1$ (estimate = 0.03, $p = \text{ns}$), but it exerted a significant impact on intention at $t = 2$ (estimate = 0.21, $p < 0.001$) (H7 supported).

Cyberloafing behavior. We earlier contended that cyberloafing intention would influence subsequent behavior. As shown in Figure 2, the effect of intention at $t = 1$ on cyberloafing behavior at $t = 2$ was significant (estimate = 0.19, $p < 0.05$), even after controlling for cyberloafing behavior at $t = 1$. This is consistent with our hypothesis (H8 supported). In addition, we proposed that past cyberloafing would have a positive impact on subsequent cyberloafing. We found that the effect of cyberloafing behavior at $t = 1$ on cyberloafing behavior at $t = 2$ was indeed strong and significant (estimate = 0.71, $p < 0.001$) (H9 supported).

Alternative Model

In addition to testing the research model, we also developed a competing model that is generally supported by past research [69, 73, 74] but represents only a part of our proposed model. Specifically, we tested partial and full models. The partial model indicates that (1) perceived risk antecedes neutralization, (2) perceived risk and neutralization affect cyberloafing intention, (3) and cyberloafing intention influences subsequent cyberloafing. Meanwhile, the full model combines the partial model with the effects of peer cyberloafing and past cyberloafing. The full model is basically the proposed model (Figure 1) plus the two paths that are supposed to be nonsignificant—that is, the relationship between neutralization and cyberloafing intention and the relationship between perceived risk and cyberloafing intention.

Table 4 shows the results of the partial and full models, including path estimates and explained variance. The fit of the partial model to the data was unsatisfactory, especially in terms of RMSEA, SRMR, and AGFI [$\chi^2(854) = 2,024.08, p < 0.001, \text{CFI} = 0.96, \text{NNFI} = 0.96, \text{RMSEA} = 0.062, \text{SRMR} = 0.118, \text{AGFI} = 0.76$]. Unsurprisingly, its fit was significantly worse than that of the proposed model, which takes into account the effects of peer cyberloafing and past cyberloafing [$\Delta\chi^2(9) = 508.14, p < 0.001$]. The average of explained variances over five factors (i.e., neutralization at $t = 1$, cyberloafing intention at $t = 1$, cyberloafing behavior at $t = 2$, neutralization at $t = 2$, cyberloafing intention at $t = 2$) was 44 percent in this partial model. This is a considerable deterioration compared with the proposed model, which explained 65 percent of the variation in research variables. We

Table 4. Results of Partial and Full Models

Causal Paths	Partial Model	Full Model
AGE → NEU1	-0.17 (0.05)***	-0.10 (0.04)*
GEN → NEU1	-0.09 (0.05)	0.01 (0.04)
SE → NEU1	0.14 (0.05)**	-0.01 (0.05)
PJ1 → NEU1	0.19 (0.05)***	0.01 (0.05)
ANG1 → NEU1	0.06 (0.05)	0.01 (0.05)
PR1 → NEU1	-0.45 (0.06)***	-0.21 (0.05)***
PC1 → NEU1		0.35 (0.06)***
CB1 → NEU1		0.41 (0.06)***
AGE → CI1	-0.10 (0.05)*	-0.02 (0.04)
GEN → CI1	-0.03 (0.04)	0.05 (0.04)
SE → CI1	0.04 (0.05)	0.02 (0.04)
PJ1 → CI1	0.10 (0.05)*	0.00 (0.04)
ANG1 → CI1	0.12 (0.05)*	0.07 (0.04)
NEU1 → CI1	0.50 (0.06)***	0.03 (0.06)
PR1 → CI1	-0.15 (0.05)**	-0.06 (0.04)
PC1 → CI1		0.15 (0.06)*
CB1 → CI1		0.71 (0.06)***
CI1 → CB2	0.75 (0.05)***	0.19 (0.08)*
CB1 → CB2		0.71 (0.09)***
AGE → NEU2	-0.03 (0.05)	-0.08 (0.04)
GEN → NEU2	-0.09 (0.05)	-0.04 (0.04)
SE → NEU2	0.14 (0.05)**	-0.01 (0.04)
PJ2 → NEU2	0.00 (0.05)	-0.10 (0.05)*
ANG2 → NEU2	0.37 (0.06)***	0.17 (0.05)***
PR2 → NEU2	-0.41 (0.05)***	-0.23 (0.05)***
PC2 → NEU2		0.43 (0.05)***
CB2 → NEU2		0.32 (0.05)***
AGE → CI2	-0.09 (0.04)*	-0.06 (0.04)
GEN → CI2	-0.06 (0.04)	-0.04 (0.03)
SE → CI2	0.10 (0.04)*	0.05 (0.04)
PJ2 → CI2	0.13 (0.04)**	0.07 (0.04)*
ANG2 → CI2	0.21 (0.05)***	0.09 (0.04)*
NEU2 → CI2	0.43 (0.05)***	0.21 (0.05)***
PR2 → CI2	-0.36 (0.05)***	0.32 (0.04)***
PC2 → CI2		0.10 (0.05)*
CB2 → CI2		0.45 (0.05)***
Explained Variance		
NEU1	0.36	0.61
CI1	0.41	0.68

(continues)

Table 4. Continued

Causal Paths	Partial Model	Full Model
Explained Variance		
CB2	0.57	0.75
NEU2	0.29	0.54
CI2	0.56	0.68

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$ (two-tailed test); standard deviations in parentheses.

Notes: AGE = age, GEN = gender, SE = self-efficacy, PJ1 = perceived justice at $t = 1$; ANG1 = anger at $t = 1$; CB1 = cyberloafing behavior at $t = 1$; PR1 = perceived risk at $t = 1$; PC1 = peer cyberloafing at $t = 1$; NEU1 = neutralization at $t = 1$; CI1 = cyberloafing intention at $t = 1$; PJ2 = perceived justice at $t = 2$; ANG2 = anger at $t = 2$; CB2 = cyberloafing behavior at $t = 2$; PR2 = perceived risk at $t = 2$; PC2 = peer cyberloafing at $t = 2$; NEU2 = neutralization at $t = 2$; CI2 = cyberloafing intention at $t = 2$.

found that neutralization was a strong antecedent of cyberloafing intention at $t = 1$ (estimate = 0.50, $p < 0.001$) and at $t = 2$ (estimate = 0.43, $p < 0.001$). Likewise, perceived risk was shown to significantly influence neutralization and cyberloafing intention at both $t = 1$ and $t = 2$, even after we controlled for control variables. Given that perceived risk and neutralization were shown to be important in determining cyberloafing intention at $t = 1$, the results of this model appear highly consistent with prior research [69, 73, 74].

Discussion

Our main objective was to study whether and (if so) how the causal relationships between the proposed antecedents and cyberloafing behavior change after the announcement of anti-cyberloafing organizational controls. To this end, we drew support from Akers's SLT and proposed a conceptual model in which neutralization, perceived risk, past cyberloafing, and peer cyberloafing served as the antecedents of cyberloafing intention. Subsequently, we developed a theoretical account of how the causal relationships between cyberloafing behavior and its antecedents change after the announcement of formal controls. We used two surveys administered one month apart in two different settings to empirically test our model. The first survey reflected the existing state of cyberloafing before the announcement of formal controls, and the second survey captured cyberloafing after the announcement of formal controls consisting of explicit monitoring and sanctions. Our results strongly supported our proposed theoretical model. In particular, we found that before the announcement of formal controls, employees' intentions to cyberloaf were mostly impacted by their past cyberloafing and their coworkers' cyberloafing behavior, but neutralization and perceived risk played no significant role. In contrast, after the announcement, neutralization and perceived risk also became significant antecedents of cyberloafing intention. Overall, our study contributes significantly to the IS literature by

emphasizing the importance of incorporating the announcement of formal controls in cyberloafing models to predict cyberloafing behavior more accurately.

Theoretical Contributions

This study is one of the first in IS research to develop and empirically validate a theoretical framework of the antecedents of cyberloafing intention before and after the announcement of formal controls. We incorporated an announcement of hypothetical organizational controls in our cyberloafing model and examined how such an announcement changes the causal relationships between cyberloafing intention and its proposed antecedents. Although our thorough literature review revealed ample research studying the antecedents of cyberloafing behavior, we could not find any earlier research that examined the changing causal relationships linking cyberloafing behavior to its proposed antecedents from before to after formal controls were put in place. Our study demonstrates that omitting the announcement of organizational controls from models of noncompliant behavior may lead to inaccurate predictions of employee conduct.

Second, our findings indicate that SLT, which proposes neutralization, perceived risk, past behavior, and peer behavior as significant antecedents of deviant behavior, can be used to explain individuals' decision making *after* the announcement of formal controls. However, it is ineffective at characterizing cyberloafing behavior *before* the announcement. Cyberloafing, as with other types of IT use, can be highly routine, and in normal situations it is not determined by deliberate evaluations of the pros and cons but rather driven by habits. Thus, we emphasize that researchers need to differentiate between deviant behavior in a routine situation and that behavior in an unusual mode. For example, we conjecture that the impact of conscious deliberation (e.g., attitude in TPB or perceived consequences in TIB) on cyberloafing behavior would not be substantial in most routine environments once its routine aspect is taken into account (e.g., past behavior or habits). Research on deviant behavior has focused on the role of risk perceptions and neutralization with the assumption that people are always sensitive to the possibility of being caught. However, this study yields valuable insights into the routine aspects of deviant behavior that have rarely been examined before.

Third, comparing the results of the partial model with those of the full model (Table 4), we demonstrated the importance of accounting for past cyberloafing and peer cyberloafing as antecedents of cyberloafing intention. The partial model reveals that before the inclusion of past cyberloafing and peer cyberloafing, neutralization and perceived risk were significant antecedents of cyberloafing intention at all times (Table 4). However, once past cyberloafing and peer cyberloafing are taken into account in the proposed full model, neutralization and perceived risk do not emerge as significant antecedents of cyberloafing intention at $t = 1$. As such, it is important to account for past cyberloafing and peer cyberloafing, along with neutralization and perceived risk, to accurately characterize cyberloafing behavior.

Fourth, by analyzing the proposed full model before and after the announcement of formal controls, we show that before the announcement neutralization and perceived risk were not significant in determining cyberloafing behavior. Instead, only employees' past cyberloafing and their coworkers' cyberloafing played a significant role in determining their intentions to cyberloaf. However, after the announcement, the impacts of neutralization and perceived risk increased in significance, but those of past cyberloafing and peer cyberloafing did not. Earlier researchers have argued that the pervasiveness of cyberloafing among coworkers leads to its normalization and in such situations cyberloafing becomes the "new norm," making it harder for organizational controls to work effectively [49]. In contrast, our findings have demonstrated that after formal controls are announced, cognitive factors—that is, neutralization and perceived risk—gain in importance, and this holds true despite controlling for past cyberloafing and peer cyberloafing.

Lastly, deterrence theory and its extended models have generally portrayed formal controls as effective deterrents against deviant behavior [26]. This view of formal controls as inhibitors of deviant behavior has been generally adopted in the IS literature in modeling IS-related counterproductive behavior, such as software piracy [31, 70] and information security violations [15, 19, 26, 33, 69, 73, 74, 81]. Meanwhile, studies like those of Galletta and Polak [29] did not find either a restrictive Internet policy or productivity control measurement effective at hindering Internet abuse. Instead, they found it is more effective than either of these to promote an organizational culture condemning the practice of cyberloafing. Moreover, Seymour and Nadasen [67] reported that subjective norms were ineffective in reducing web abuse and that, surprisingly, managerial supervision had the unexpected effect of increasing web abuse. In agreement with deterrence theory, our results indicated that cyberloafing intention decreased significantly overall (mean of CI1 = 4.7; mean of CI2 = 3.8). However, we add to the literature on deterrence and IS violations by empirically demonstrating that the effects of formal controls on cyberloafing behavior in organizations are more complex than was known in the literature.

Specifically, as noted earlier, factors such as neutralization and perceived risk that previously were not significantly related to cyberloafing intention suddenly became significant after the announcement of formal controls. Thus, the announcement of formal controls activates the deterring influence of perceived risk on cyberloafing, but it also has the undesired effect of simultaneously actuating neutralization. This increased significance of neutralization after the announcement of formal controls has often been neglected in studies on cyberloafing behavior [47, 57, 79]. Equally important, other notable evaluations, both cognitive (e.g., perceived justice) and emotional (e.g., anger), also unexpectedly turned into significant precursors of cyberloafing intention after formal controls were announced. An important implication of these findings is that we learn more about how formal controls operate when potentially changing behavior is the issue. Specifically, this study suggests that formal controls may help reduce cyberloafing intention in general, but at the cost of a tendency to make employees highly aware of the unsatisfactory conditions

within their work environment. Thus, our results emphasize the importance of incorporating the announcement of formal controls into cyberloafing models to better explain the varying effects of the antecedents of cyberloafing behavior.

Managerial Implications

The results of this study may increase managers' awareness of the repercussions of not enforcing anti-cyberloafing controls in their organizations as well as the expected changes in employee behavior after an announcement of such controls. We identify the antecedents of cyberloafing intention—neutralization, perceived risk, past cyberloafing, and coworkers' cyberloafing—and, as such, suggest effective strategies to thwart cyberloafing. We found it especially imperative that organizations discourage their employees from neutralizing their guilt and downplaying the negative connotations and repercussions of their cyberloafing. By further uncovering the antecedents of neutralization, our study suggests the following practical ways to curb employees' neutralization tendencies and cyberloafing intentions.

First, we found that increasing employees' perceived risk is one way of dampening neutralization and deterring cyberloafing. Imposing sanctions associated with concrete and measurable punishments has been shown to increase perceived risk [19, 31, 38, 69, 73, 74]. This is because such formal sanctions are often accompanied by measurable losses (e.g., loss of bonus) [38], and, as suggested by prior research, rational individuals tend to engage in an activity only if they expect benefits that outweigh potential losses [19]. Importantly, being singled out and punished often results in social stigma and shame that can be as devastating as material losses. Further, although perceived risk was found to mitigate neutralization tendencies before and after the announcement of formal controls, it only became effective at deterring cyberloafing intention after formal controls were announced. In other words, perceived risk without formal controls might be effective at decreasing neutralization but will not necessarily be reflected in an effectual decrease in employees' intention to cyberloaf. This subtle but important distinction is additional proof of the importance of imposing formal controls.

Second, our results established that past cyberloafing and cyberloafing by coworkers are associated with a significant increase in neutralization. Further, an important finding from our study is that without formal controls, cyberloafing tends to be perpetuated among past cyberloafers and spread to noncyberloafers. Given that cyberloafers are expected to blame their behavior on others' unpunished cyberloafing, it is important for organizations to impose sanctions on cyberloafers and show everyone in the organization that violators will be apprehended and punished. To ensure that all employees are fully aware of the risks of cyberloafing, organizations need to announce and communicate formal controls to everyone in the organization. Further, to ensure that everyone understands the new policy and the consequences of violating it, employees could undergo scenario-based exercises as part of a comprehensive training program [16, 32, 69].

Lastly, Siponen and Vance [69, p. 498] argued that “formal sanctions serve an important role in the implementation and enforcement of IS security policies.” In contrast, our results suggest that imposing formal controls can unexpectedly backfire because neutralization, perceived risk, perceived justice, and anger, which are deemed strongly correlated with employee morale [35], become significantly related to cyberloafing intention after the announcement of formal controls. Thus, in order to boost employees’ morale, managers in organizations may need to clearly communicate and explain the rationale behind their imposing formal controls. Such explanations can make employees feel more engaged in the decision-making process, which could in turn dampen negative feelings and their expected negative repercussions. In addition to being significant in determining cyberloafing intention after the announcement of formal controls, factors such as neutralization, perceived justice, perceived risk, and anger have also been blamed for decreases in organizational citizenship behavior, prosocial behavior, and job satisfaction [58], and for increased retaliatory behavior [25, 63]. Thus, managers need to understand that the announcement of formal controls may ignite unexpected backfiring that could harm the performance of their business as a whole [25, 27, 48, 58, 62, 63].

Limitations and Future Directions

Several limitations of our study need to be mentioned. We attempted to include in our conceptual model the research and control variables that are most relevant to the study of cyberloafing behavior. However, it is still possible that some important factors remain unaccounted for. For example, this study did not include factors related to firm–employee relationships. It also did not account for the types of controls actually implemented in the respondents’ organizations; thus, the impact of formal controls on cyberloafing behavior is likely to be less influential for those previously exposed to formal controls than for those without any prior experience with formal controls. Future research needs to more thoroughly validate our model by using additional variables that could be vital in the context of cyberloafing behavior. Meanwhile, it is important to note that our results may not be completely free from CMV. Thus, care should be taken in interpreting our findings. Another limitation relates to the hypothetical scenario method used in this study. Hypothetical scenarios have been widely accepted in IS security privacy research [15, 22]. In addition, the participants of the present study considered our scenario fairly realistic. However, our model should be further validated through field studies with actual organizational controls.

Moreover, we did not study factors related to how the announcement of organizational controls is handled such as, for example, the perceived fairness of the way the announcement is delivered to employees. In a similar vein, we did not consider organizational controls with varying levels of severity. Differentiating between organizational controls of various degrees of fairness and of varying levels of severity could lead to different results. Thus, our findings cannot be generalized to

settings other than the one examined in this study. Finally, an additional limitation pertains to our conceptualization of the neutralization construct. In choosing the neutralization techniques that apply to the context of our study, we selected those that are most often examined in the context of cyberloafing. However, although prior work has typically omitted neutralization techniques that were deemed less applicable to certain contexts [4], the possibility exists that some important elements of neutralization have been overlooked.

This study opens the door for exciting and fertile research directions. First of all, it focused on individuals' immediate reactions to the announcement of organizational controls, but it did not examine how such reactions persist over time. Additional research is necessary to understand whether and, if so, how quickly the effects of organizational controls would vanish completely. For example, to assess the effects of controls that may vary over time, researchers can collect proximal reactions from one subgroup (e.g., immediately after the announcement of formal controls) and distal reactions from another group (e.g., two months after the announcement). In this way, researchers would be able to better understand the role of the passage of time in organizational controls.

Further, it would be beneficial to investigate what type of justice perceptions—distributive, procedural, or interactional—affect neutralization the most. Prior studies have identified other predictors of cyberloafing behavior, including the lack of organizational commitment, work boredom and lack of involvement, and a lax organizational culture [47, 79]. Our conceptual framework can easily accommodate such additional variables, and we hope that further research extends our model to include some of these additional factors and studies the interactional effects among them.

This study shows that perceived justice and anger play an important role in determining neutralization and cyberloafing intention, and especially after the announcement of formal controls. Perceived justice and anger represent, respectively, the cognitive and emotional factors relevant to cyberloafing behavior [23, 59, 65]. In this study, these variables were conceptualized as control variables because they do not fit neatly into SLT. However, given their significance, perceived justice and anger could be better treated as main variables in a research model. Our findings call for more careful theoretical work that leads to the integration of the cognitive and emotional factors into the larger framework of SLT in the context of cyberloafing behavior.

In addition, our findings indicate that perceived risk is an important predictor of neutralization and cyberloafing intention, especially after the announcement of formal controls. Although this study examined the effects of perceived risk on cyberloafing behavior, it did not examine the antecedents of these risk perceptions. Research suggests that trust plays an important role in determining perceived risk [54]. Thus, we encourage researchers to take into account trust and other potential antecedents of perceived risk to better understand the nature of perceived risk in the context of cyberloafing behavior.

Although this study has suggested ways to thwart future cyberloafing intention, it did not address the ultimate effect on employees' loyalty and productivity. This research can also be extended to study the effect of neutralization and its antecedents on employee loyalty and productivity after the announcement of formal controls. For example, although perceived justice was found to reduce neutralization, it could, in the process, reduce loyalty after the announcement. Accounting for postloyalty and postproductivity is important to draw a more complete, practical picture. More effort needs to be exerted to understand the complexities of employees' perceptions and behavior after the announcement. We hope that our model has provided a solid theoretical foundation for extended research in this important area.

Conclusions

This article reports the first study to develop and test a theoretical framework of the changing causal relationships between cyberloafing behavior and its antecedents before and after the announcement of formal controls. Our findings generally suggest that neutralization, perceived risk, past cyberloafing, and peer cyberloafing should all be taken into consideration to accurately predict employees' cyberloafing intentions. What is especially important and contrary to common belief is that after past cyberloafing and peer cyberloafing are introduced in our model, neutralization and perceived risk became significant antecedents of cyberloafing intention only after the announcement of formal controls. Overall, this work contributes to IS research by elucidating how the announcement of formal organizational controls changes the causal relationships between cyberloafing behavior and its antecedents. We believe that our model is applicable to other behavioral research that investigates people's deviances and to research investigating the effectiveness of organizational controls in various organizational and societal contexts. We hope that our model constitutes a strong theoretical foundation for future research in workplace deviance and criminology.

Acknowledgments: The authors are very grateful to *JMIS* Editor-in-Chief, Professor Zwass, the anonymous associate editor, and the three anonymous referees for their valuable insights.

Funding

This research was funded, in part, by a grant from the European Regional Development Fund (ERDF) and the Finnish Funding Agency for Innovation.

Supplemental File

Supplemental data for this article can be found on the publisher's website at [10.1080/07421222.2017.1297173](https://doi.org/10.1080/07421222.2017.1297173)

NOTES

1. It is noteworthy that some studies have found benefits to nonwork-related computing such as improved workplace productivity [24]. However, our focus in this study is not on the repercussions of cyberloafing but on the antecedents of cyberloafing intention.

2. Close monitoring and punishment are rare, but nevertheless, they do exist [49]. Thus, we consider the formal controls described in the scenario realistic. In order to formally check the realism of the scenario, we used a one-item seven-point scale ranging from 1 (strongly disagree) to 7 (strongly agree). We found that the average score for realism was 5.00, which suggests that participants considered the scenario realistic.

3. One might argue that the differences in structural relationships between the pre- and postannouncement periods result from the mere fact that respondents were shown the same items twice and thus changed the way they reacted to the items. In order to exclude this alternative explanation, we collected data as a control group ($n = 150$). The results indicated that in the absence of a scenario, the responses of this control group to both surveys were almost identical. Thus, it is safe to rule out methodological artifacts as an explanation for the differences in structural relationships observed in the present study. Please refer to Online Appendix B for more information on the results of the control group.

4. An important assumption of this study was that organizational controls after the announcement are stricter than those before such an announcement. Accordingly, we expected that the interventions described in the hypothetical scenarios would be stricter than those generally practiced in actual organizations. We collected additional data to see if this assumption holds true and whether the results of the model would stay the same even after controlling this extra information. In particular, we replicated Survey 1 with two additional questions concerning existing organizational interventions ($n = 265$). The results indicated that our scenario indeed represents an extreme form of controls as compared with current practices in actual organizations. We also found that the existing levels of monitoring and punishment do not have any significant effect on neutralization and cyberloafing intention. Finally, the results of our hypotheses were shown to stay exactly the same even after controlling for the existing levels of monitoring and punishment. Online Appendix C describes the new data collection procedure and shows the results of the ad hoc analyses.

ORCID

Lara Khansa  <http://orcid.org/0000-0001-7305-5190>

REFERENCES

1. Aghaz, A., and Sheikh, A. Cyberloafing and job burnout: An investigation in the knowledge-intensive sector. *Computers in Human Behavior*, 62, (2016), 51–60.
2. Ajzen, I. From intentions to actions: A theory of planned behavior. In J. Kuhl and J. Beckman (eds.), *Action Control: From Cognition to Behavior*. New York, NY: Springer-Verlag, 1985, pp. 11–39.
3. Akers, R.L. *Deviant Behavior: A Social Learning Approach*, 2nd ed. Belmont, CA: Wadsworth, 1977.
4. Akers, R.L.; Krohn, M.D.; Lanza-Kaduce, L.; and Radosevich, M. Social learning and deviant behavior: A specific test of a general theory. *American Sociological Review*, 44, 4 (1979), 636–655.
5. Akers, R.L., and Sellers, C.S. *Criminological Theories: Introduction, Evaluation, and Application*, 4th ed. Los Angeles, CA: Roxbury Press.
6. Anderson, B.B.; Vance, A.; Kirwan, C.B.; Jenkins, J.L.; and Eargle, D. From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems*, 33, 3 (2016), 713–743.

7. Anderson, C.L., and Agarwal, R. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34, 3 (2010), 613–643.
8. Anderson, J.C., and Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103, 3 (1988), 411–423.
9. Bagozzi, R.P., and Yi, Y. On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16, 1 (1988), 74–94.
10. Bandura, A. *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice Hall, 1986.
11. Barnett, J., and Breakwell, G.M. Risk perception and experience: Hazard personality profiles and individual differences. *Risk Analysis*, 21 (2001), 171–177.
12. Bearden, W.O.; Netemeyer, R.G.; and Mobley, M.F. *Handbook of Marketing Scales: Multi-item Measures for Marketing and Consumer Behavior Research*. Newbury Park, CA: Sage, 1993.
13. Blau, P.M. *Exchange and Power in Social Life*. New York, NY: Wiley, 1964.
14. Bock, G.-W.; Park, S.C.; and Zhang, Y. Why employees do non-work-related computing in the workplace. *Journal of Computer Information Systems*, 50, 3 (2010), 150–163.
15. Boss, S.R.; Galletta, D.F.; Lowry, P.B.; Moody, G.D.; and Polak, P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39, 4 (2015), 837–864.
16. Burns, A.J.; Posey, C.; Roberts, T.L.; and Lowry, P.B. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68 (2017), 190–209.
17. Chang, M.K., and Cheung, W. Determinants of the intention to use Internet/WWW at work: A confirmatory study. *Information and Management*, 39, 1 (2001), 1–14.
18. Chatterjee, S.; Sarker, S.; and Valacich, J.S. The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, 31, 4 (2015), 49–87.
19. Chen, Y.; Ramamurthy, K.; and Wen, K.-W. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29, 3 (Winter 2012–13), 157–188.
20. Cheung, W.; Chang, M.K.; and Lai, V.S. Prediction of internet and world wide web usage at work: A test of an extended Triandis model. *Decision Support Systems*, 30, 1 (2000), 83–100.
21. Chin, W.W.; Gopal, A.; and Salisbury, W.D. Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation. *Information Systems Research*, 8, 4 (1997), 342–367.
22. Choi, B.C.; Jiang, Z.J.; Xiao, B.; and Kim, S.S. Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, 24, 4 (2015), 675–694.
23. Choi, B.C.; Kim, S.S.; and Jiang, Z.J. Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, 33, 3 (2016), 904–933.
24. Coker, B.L. Workplace Internet leisure browsing. *Human Performance*, 26, 2 (2013), 114–125.
25. D'Arcy, J.; Herath, T.; and Shoss, M.K. Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31, 2 (2014), 285–318.
26. D'Arcy, J.; Hovav, A.; and Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20, 1 (2009), 79–98.
27. Dennis, A.R.; Robert, L.P., Jr.; Curtis, A.M.; Kowalczyk, S.T.; and Hasty, B.K. Research note—Trust is in the eye of the beholder: A vignette study of postevent behavioral controls' effects on individual trust in virtual teams. *Information Systems Research*, 23, 2 (2012), 546–558.

28. Fornell, C., and Larcker, D.F. Structural equation models with unobservable variables and measurement errors. *Journal of Marketing Research*, 18, 3 (1981), 39–50.
29. Galletta, D.F., and Polak, P. An empirical investigation of antecedents of Internet abuse in the workplace. In *Proceedings of the Second Annual Workshop on HCI Research in MIS*. Seattle, WA, 2003, pp. 12–13.
30. Gefen, D.; Straub, D.; and Boudreau, M. Structural equation modeling and regression: Guidelines for research practice. *Communications of the AIS*, 4, 7 (2000), 1–77.
31. Gopal, R., and Sanders, G. Preventive and deterrent controls for software piracy. *Journal of Management Information Systems*, 13, 4 (Spring 1997), 29–47.
32. Guo, H.; Cheng, H.K.; and Kelley, K. Impact of network structure on malware propagation: A growth curve perspective. *Journal of Management Information Systems*, 33, 1 (2016), 296–325.
33. Guo, K.H.; Yuan, Y.; Archer, N.P.; and Connelly, C.E. Understanding non-malicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28, 2 (Fall 2011), 203–236.
34. Harrington, S.J. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, 20, 3 (1996), 257–278.
35. Hsu, J.S.-C.; Shih, S.-P.; Hung, Y.W.; and Lowry, P.B. The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, 26, 2 (2015), 282–300.
36. Hu, L.T., and Bentler, P.M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6, 1 (1999), 1–55.
37. Hu, Q.; West, R.; and Smarandescu, L. The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, 31, 4 (2015), 6–48.
38. Johnston, A.C.; Warkentin, M.; and Siponen, M.T. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39, 1 (2015), 113–134.
39. Jöreskog, K., and Sörbom, D. *LISREL8: User's Reference Guide*. Chicago, IL: Scientific Software International, 1996.
40. Khansa, L.; Ma, X.; Liginlal, D.; and Kim, S.S. Understanding members' active participation in online question-and-answer communities: A theory and empirical analysis. *Journal of Management Information Systems*, 32, 2 (2015), 162–203.
41. Kim, S.S., and Malhotra, N.K. A longitudinal model of continued IS use: An integrative view of four mechanisms underlying postadoption phenomena. *Management Science*, 51, 5 (2005), 741–755.
42. Kim, S.S., and Son, J.Y. Out of dedication or constraint? A dual model of post-adoption phenomena and its empirical test in the context of online services. *MIS Quarterly*, 33, 1 (2009), 49–70.
43. Klockars, C.B. *The Professional Fence*. New York, NY: Free Press, 1974.
44. Koklic, M.K.; Kukar-Kinney, M.; and Vida, I. Three-level mechanism of consumer digital piracy: Development and cross-cultural validation. *Journal of Business Ethics*, 134, 1 (2014), 1–13.
45. Liang, H.; Xue, Y.; and Wu, L. Ensuring employees' IT compliance: Carrot or stick? *Information Systems Research*, 24, 2 (2013), 279–294.
46. Liang, N.; Biros, D.P.; and Luse, A. An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, 33, 2 (2016), 361–392.
47. Liberman, B.; Seidman, G.; McKenna, K.Y.A.; and Buffardi, L.E. Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Computers in Human Behavior*, 27, 6 (2011), 2192–2199.
48. Lim, V.K.G. The IT way of loafing on the job: Cyberloafing, neutralizing, and organizational justice. *Journal of Organizational Behavior*, 23, 5 (2002), 675–694.
49. Lim, V.K.G., and Teo, T.S.H. Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information and Management*, 42 (2005), 1081–1093.

50. Limayem, M., and Hirt, S. How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly*, 31, 4 (2007), 705–737.
51. Lindell, M.K., and Whitney, D.J. Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86, 1 (2001), 114–121.
52. Lowry, P.B.; Zhang, J.; Wang, C.; and Siponen, M. Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research*, 27, 4 (2016), 962–986.
53. Ma, X.; Khansa, L.; Deng, Y.; and Kim, S.S. Impact of prior reviews on the subsequent review process in reputation systems. *Journal of Management Information Systems*, 30, 3 (Winter 2014), 279–310.
54. Malhotra, N.K.; Kim, S.S.; and Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15, 4 (2004), 336–355.
55. Malhotra, N.K.; Kim, S.S.; and Patil, A. Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, 52, 12 (2006), 1865–1883.
56. Minor, W.W. Neutralization as a hardening process: Considerations in the modeling of change. *Social Forces*, 62 (1984), 995–1019.
57. Moody, G.D., and Siponen, M. Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information and Management*, 50 (2013), 322–335.
58. Niehoff, B.P., and Moorman, R.H. Justice as a mediator of the relationship between methods of monitoring and organizational citizenship behavior. *Academy of Management Journal*, 36, 3 (1993), 527–556.
59. Nyer, P.U. A study of relationships between cognitive appraisals and consumption emotions. *Journal of the Academy of Marketing Science*, 25, 4 (1997), 296–304.
60. O'Guinn, T.C., and Faber, R.J. Compulsive buying: A phenomenological exploration. *Journal of Consumer Research*, 16 (September 1989), 147–157.
61. Pee, L.G.; Woon, I.M.Y.; and Kankanhalli, A. Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information and Management*, 45 (2008), 120–130.
62. Piccoli, G., and Ives, B. Trust and the unintended effects of behavior control in virtual teams. *MIS Quarterly*, 27, 3 (2003), 365–395.
63. Posey, C.; Bennett, R.; Roberts, T.L.; and Lowry, P.B. When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, 7, 1 (2011), 24–47.
64. Ronis, D.L.; Yates, J.F., and Kirscht, J.P. Attitudes, decisions, and habits as determinants of repeated behavior. In A.R. Pratkanis, S.J. Breckler, and A.G. Greenwald (eds.), *Attitude Structure and Function*. Hillsdale, NJ: Lawrence Erlbaum, 1989, pp. 213–239.
65. Schmidt, T.A.; Houston, M.B.; Bettencourt, L.A.; and Boughton, P.D. The impact of voice and justification on students' perceptions of professors' fairness. *Journal of Marketing Education*, 25, 2 (2003), 177–186.
66. Segars, A.H. Assessing the unidimensionality of measurement: A paradigm and illustration within the context of information systems research. *Omega*, 25, 1 (1997), 107–121.
67. Seymour, L., and Nadasen, K. Web access for IT staff: A developing world perspective on web abuse. *Electronic Library*, 25, 5 (2007), 543–557.
68. Sheeran, P. Intention-behaviour relations: A conceptual and empirical review. *European Review of Social Psychology*, 12 (2002), 1–36.
69. Siponen, M., and Vance, A. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34, 3 (2010), 487–502.
70. Siponen, M.; Vance, A.; and Willison, R. New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information and Management*, 49, 7 (2012), 334–341.

71. Smith, K.J.; Davy, J.A.; and Easterling, D. An examination of cheating and its antecedents among marketing and management majors. *Journal of Business Ethics*, 50, 1 (2004), 63–80.
72. Son, J.-Y., and Kim, S.S. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32, 3 (2008), 503–529.
73. Straub, D.W. Effective IS security: An empirical study. *Information Systems Research*, 1, 3 (1990), 255–276.
74. Straub, D.W., and Nance, W.D. Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 14, 1 (1990), 45–60.
75. Taylor, S., and Todd, P.A. Understanding information technology usage: A test of competing models. *Information Systems Research*, 6, 2 (June 1995), 144–176.
76. Triandis, H.C. Values, attitudes, and interpersonal behavior. In M.M. Page (ed.), *Nebraska Symposium on Motivation 1979—Beliefs, Attitudes and Values*. Lincoln, NE: University of Nebraska Press, 1980, pp. 195–260.
77. Vance, A.; Lowry, P.B.; and Eggett, D. Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29, 4 (2013), 263–290.
78. Venkatesh, V., and Davis, F.D. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46, 2 (2000), 186–204.
79. Vitak, J.; Crouse, J.; and LaRose, R. Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, 27, 5 (2011), 1751–1759.
80. Wagner, D.T.; Barnes, C.M.; Lim, V.K.G.; and Ferris, D.L. Lost sleep and cyberloafing: Evidence from the laboratory and a daylight saving time quasi-experiment. *Journal of Applied Psychology*, 97, 5 (2012), 1068–1076.
81. Zobel, C.W., and Khansa, L. Quantifying cyberinfrastructure resilience against multi-event attacks. *Decision Sciences*, 43, 4 (2012), 687–710.

Appendix A: Measures and Scenarios

Cyberloafing behavior (CB)

- On average, how frequently have you used the Internet at work for nonwork-related purposes over the past month? (1 = less than once a week; 2 = a few times a week; 3 = about one a day; 4 = a few times a day; 5 = once an hour; 6 = several times an hour).
- I have frequently used the Internet at work for nonwork-related purposes on a typical day.

Perceived risk (PR)

- I consider cyberloafing dangerous.
- Cyberloafing would put me in jeopardy.
- It is risky for me to engage in cyberloafing.
- Cyberloafing would eventually cause problems for me.

Peer cyberloafing (PC)

- I believe most people occasionally engage in cyberloafing.
- I am convinced my coworkers occasionally engage in cyberloafing.

Neutralization (NEU)

- It is acceptable to engage in cyberloafing if no harm is done to the company.
- Hard work can compensate for engaging in cyberloafing.
- If a person gets the job done, it is all right to occasionally engage in cyberloafing.

Cyberloafing intention (CI)

- I predict that I would use the Internet at work for nonwork-related purposes in the next month.
- I intend to use the Internet at work for nonwork-related purposes in the next month.
- I plan to use the Internet at work for nonwork-related purposes in the next month.

Self-efficacy (SE)

- It is easy for me to use information technologies in general (e.g., computers, smartphones).
- I have the skill to use information technologies in general (e.g., computers, smartphones).
- I am able to proficiently use information technologies in general (e.g., computers, smartphones).

Perceived justice (PJ)

- My company is fair in dealing with cyberloafing.
- My company's policy related to cyberloafing is reasonable.
- In general, cyberloafing is handled reasonably in my company.

Anger (ANG) (seven-point scales ranging from "not at all" to "to a great extent")

- Furious
- Irritated
- Angry

Note: Unless otherwise indicated, the anchors for all items were 1 = strongly disagree to 7 = strongly agree.

Scenario

In the scenario, your company has just announced through e-mail a new policy to address the problem associated with cyberloafing. The scenario reads as follows: "It has come to our attention that some employees have been using the Internet and other information technologies for nonwork-related purposes.

From now on, the company will closely keep track of your use of the Internet and other information technologies (e.g., e-mails, social networking services, online news, software downloads, and financial transactions) within its physical and virtual confines.

Cyberloafing will result in disciplinary actions up to and including *termination of employment*."

Demographic information

- Age: (Years old)
 - Gender: (1 = male; 2 = female)
-