24 The Dark Side of Workplace Technology

Cyber-Related Counterproductive Work Behavior, Workplace Mistreatment, and Violation of Workplace Ethics

David J. Howard and Paul E. Spector

There is perhaps no workplace factor that has a bigger negative impact on employee behavior than technology. Technology has had a monumental impact on both the physical aspects of the workplace and how workers perform their jobs, transitioning from a largely paper-and-pencil office to the computerized world we live in today that can allow for more efficient performance of job tasks and the ability to work remotely. Furthermore, information and communication technologies (ICT) have changed the way that people behave and communicate in the workplace. ICT advances have created new devices and media for interactions among employees and between employees and the public (e.g., customers). At the same time, electronic access to organizational and personal information has created the means for employees to intentionally or unintentionally misuse ICT devices and an organization's sensitive data. Thus, these technologies have provided new opportunities for organizational insiders and outsiders to engage in counterproductive work behavior (CWB; behavior that harms organizations or people in organizations), and unethical behaviors, including workplace mistreatment.

The workplace mistreatment literature falls within the domain of occupational health psychology, linking workplace experience to employee health and wellbeing. The proliferation of the Internet and ICT usage in today's changing workplace has led to new cyber-occupational health psychology (C-OHP) constructs being studied, including cyber incivility and cyberbullying. CWB research focuses on the actor's behavior, with much of it concerned with the impact of these behaviors on organizational functioning. Again, we find that technology has created new opportunities for employees to engage in cyber-CWB (C-CWB) with behaviors like cyberloafing, cyber-sabotage, and cyber-theft. This chapter has three goals: (1) to present a brief overview of counterproductive work behaviors and workplace mistreatment, (2) review the current literature that focuses on newer technology-driven C-CWB and C-OHP constructs, and (3) to discuss the ethical implications involved with organizations attempting to minimize C-CWB using workplace monitoring methods.

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

Counterproductive Work Behaviors and Workplace Mistreatment

Counterproductive work behaviors (CWBs) are intentional acts that harm or are intended to harm the organization or people in organizations (Spector & Fox, 2005). The definition of CWB reveals the boundary condition that the behavior must be a volitional act, one that the employee purposefully commits. For example, if an employee's assigned workload was too high for him or her to be able to complete all tasks, that employee would not be committing a CWB if failing to complete a task because his or her intention was to complete their assigned work, but the workload level made it impossible. However, if the same employee was sabotaging a team's production tasks so they were unable to complete their work, then the employee would be committing a CWB. Additionally, there is no boundary condition with regard to intent to harm; only that the purposeful behavior, either directly or indirectly, harms the organization or coworkers (Jex & Britt, 2014, p. 178). Unless the behavior is accidental (a common occurrence in cybersecurity behaviors discussed later in the chapter), if subsequent harm occurs to a coworker or the organization, it is considered a CWB.

Workplace mistreatment occurs when an employee experiences a harmful physical (e.g., being hit) or psychological (e.g., being yelled at) incident at work (Cortina & Magley, 2003, p. 247). Similar to CWB, workplace mistreatment is an overarching term used to describe a variety of behaviors that have negative effects on workers and organizations. Workplace mistreatment constructs generally examined from the target's perspective include abusive supervision, bullying, incivility, interpersonal conflict, and social undermining (Hershcovis, 2011), and the constructs are typically differentiated by the frequency, intensity or severity, and intentionality of the behaviors. Workplace bullying (sometimes referred to as mobbing) is the persistent exposure to interpersonal aggression and mistreatment from supervisors, subordinates, or colleagues (Einarsen, Hoel, & Notelaers, 2009) from which they have difficulty defending themselves (Yang, Caughlin, Gazica, Truxillo, & Spector, 2014), including abuse, ridicule, teasing, and social exclusion (Einarsen, 2000). The frequency and at times escalating nature of the hostile coworker relationship is one of the defining characteristics of bullying (Einarsen et al., 2009), and may also occur in conjunction with a power imbalance among organization members (Hershcovis, 2011; Niedl, 1996). Because the targets of bullying often feel defenseless and are subject to harassment for extended periods of time, the outcomes of bullying can be severe and long-lasting, impacting the victim's mental health and well-being (Van den Brande, Baillien, De Witte, Vander Elst, & Godderis, 2016) as well as organizational outcomes such as turnover, worker's compensation and litigation (Hoel, Sheehan, Cooper, & Einarsen, 2011).

Workplace incivility refers to "rude, condescending, and ostracizing acts that violate workplace norms of respect, but otherwise appear mundane" (Cortina, Kabat-Farr, Magley, & Nelson, 2017, p. 299). Workplace incivility is a low

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

intensity behavior and may be limited to a single event. Unlike other CWB/ mistreatment constructs, employees who commits uncivil acts might not realize their actions were interpreted by coworkers in this manner, nor did they necessarily intend to cause harm to others. Perhaps because of this, the prevalence of workplace incivility is extremely high, with as many as 98% of employees reporting having been the recipient of workplace incivility at some point, and nearly half reporting incivility on a weekly basis (Porath & Pearson, 2013). The negative outcomes associated with being the target of workplace incivility are far-reaching, including affective (e.g., anger and other emotions), cognitive (e.g., lower motivation and perceptions of fairness), and behavioral (e.g., retaliation) effects (Schilpzand, de Pater, & Erez, 2016). Furthermore, Andersson and Pearson's (1999) work reports an escalating "tit-for-tat" among coworkers occurring with workplace incivility.

C-CWB and Workplace Mistreatment

Tepper's (2000) seminal article "Consequences of abusive supervision" begins with the following quote from the 1994 film *Swimming with Sharks*, starring Kevin Spacey as an abusive supervisor and Frank Whaley as his assistant:

> "What did I tell you the first day? Your thoughts are nothing; you are nothing ... if you were in my toilet bowl I wouldn't bother flushing it. My bath mat means more to me than you ... you don't like it here, leave!"

The quote is shocking in its display of behavior from one organization member toward another and the movie is filled with abusive supervision, bullying, incivility, and retaliation. However, a viewing of the film today proves just how much the workplace has changed in the past two decades. No longer is wearing a wired headset for one's work phone considered an extravagant luxury, and no longer are employees using pay phones to return phone calls to a number sent on a pager. The employee of today is often contacted through email and text message, both during work hours and away from the office, and it is commonplace for employees to use laptops and smartphones for work. Personal computers and other ICT devices have thoroughly changed the workplace of today, allowing for more efficiency and productivity, but at the same time these technologies present the opportunity for employees to engage in new forms of C-CWB and worker mistreatment. This chapter reviews the literature for four of these behaviors: cyberloafing, cyber incivility, cyberbullying, and insider threats to cybersecurity.

Cyberloafing

Each spring, the National Collegiate Athletic Association (NCAA) hosts the Division 1 basketball tournament known as March Madness, where 68 teams from colleges and universities around the United States vie to be crowned that season's champion. The tournament is a widely viewed affair that has

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

increasingly been streamed by workers online, as many of the games occur during regular workday hours on Thursday and Friday for two consecutive weeks. Challenger, Gray & Christmas (2016) estimate the total loss to organizations from their employees' lost productivity regarding the 2016 March Madness tournament approaches $4 billion. It is easy to understand the concern that employers have regarding their employees' personal Internet usage during work, as the current total estimated costs to US businesses approaches $85 billion annually (Zakrzewski, 2016). The ubiquity of Internet access through smartphones, combined with the popularity of social networking websites (e.g., Facebook, Instagram, Twitter) and websites such as YouTube, Reddit, E-bay, and Amazon, has forced organizations to consider how to manage their employees' cyberloafing habits.

Cyberloafing is an employee's voluntary usage of the Internet to engage in non-work-related web browsing and personal email communication during office hours (Lim, 2002). In recent years, cyberloafing has become pervasive in the workplace, with up to 90% of employees admitting to browsing the Internet for personal use while at work (Lim & Teo, 2005) and 96% receiving personal email during work (Blanchard & Henle, 2008). Cyberloafing behaviors have been classified into two broad categories: minor cyberloafing (e.g., checking personal email at work, browsing news websites) and serious cyberloafing (e.g., online gaming and gambling, visiting adult-oriented websites), with the percentage of workers committing serious cyberloafing infractions fewer than those who commit minor behaviors (Blanchard & Henle, 2008).

While there is agreement in the extant literature that cyberloafing is a CWB, there is disagreement regarding to which CWB category cyberloafing belongs. Lim (2002) originally categorized cyberloafing as a form of production deviance ("purposeful failure to perform job tasks effectively the way they are supposed to be performed," Spector et al., 2006, p. 449) because of the relatively minor nature of cyberloafing compared to more severe CWBs such as sabotage, and this classification remains popular among researchers (e.g., Blanchard & Henle, 2008; Restubog et al., 2011). Alternately, cyberloafing has been described as a withdrawal construct (Askew et al., 2014). Withdrawal behaviors are those that reduce the amount of time worked that is required by the organization (Spector et al., 2006) and include arriving late to work, taking longer lunch breaks than allowed, and leaving early (Krischer, Penney, & Hunter, 2010). Research shows that the average amount of time workers spend on cyberloafing varies from around one hour to half the day, and it is clear that when employees are using the Internet for their personal use they are not performing the job as the organization requires. Further evidence for cyberloafing as a withdrawal behavior exists with its significant correlation with lateness, absenteeism, extended breaks, and leaving early (Askew et al., 2014). We agree with Askew et al. (2014) that cyberloafing more closely aligns with withdrawal behaviors.

Much like other CWBs, it is important for organizations to be able to understand the mechanisms behind why people cyberloaf when they should be performing their duties. The theory of planned behavior (TPB) has emerged as a

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

theoretical framework to study cyberloafing. While emotion-based theories and models have dominated research to examine reactive CWBs (i.e. CWBs resulting from negative emotions caused by one's work environment), TPB can be particularly useful in examining the nature of instrumental CWBs. Instrumental CWBs are "based primarily on "cold" cognitions, plans, and personal or professional strategies, as opposed to "hot" emotions and associated cognitive processes" (Fox & Spector, 2010, p. 94). TPB states that social norms, attitudes, and perceived behavioral control lead to behavior through intentions (Ajzen, 1985). The norms in an organizational context are behaviors considered acceptable among coworkers, even though the behavior may not be officially condoned by the company, and social norms have proven to be one of the best predictors of cyberloafing (e.g., Askew et al., 2014; Blanchard & Henle, 2008; Restubog et al., 2011). Lim and Chen (2012) found employees thought cyberloafing for 75 minutes a day was an acceptable amount and often employees feel that their web browsing habits do not affect the organization, nor are their browsing habits dissimilar from their coworkers'. Cyberloafing attitudes in the TPB model can be measured by asking workers how they feel about cyberloafing, for example, with items from Askew et al. (2014) asking "participants to rate the extent to which they think cyberloafing is valuable, enjoyable, beneficial, and good" (p. 514).

In addition to directly asking respondents their attitudes about cyberloafing, other attitudinal variables, such as job involvement (Liberman, Seidman, McKenna, & Buffardi, 2011) and organizational justice (Lim, 2002), have also been found to predict cyberloafing. When considering why workers cyberloaf and their perceived control with regard to browsing the Internet at work, one cannot help but think that sometimes the answer is the most obvious one: they cyberloaf because they can. Even in the early twenty-first century, Internet access at work was largely able to be monitored and controlled by information technology (IT) departments. However, the rise of smartphone technology and unlimited data plans gives workers easy access to the Internet without having to use their employer's Internet connection. The ability to loaf is even greater if the employee is not being closely monitored (a topic we will cover more at length at the end of this chapter) and many workers can make it look like they are working while they browse the Internet on their work PC (Lim & Teo, 2005). The physical transformation of the workplace to now include teleworkers (working from home or away from the office) has allowed cyberloafing to flourish, and O'Neill, Hambley, and Bercovich (2014) find cyberloafing behaviors to negatively relate to job satisfaction for these workers.

Not all researchers believe that cyberloafing is entirely bad for organizations though, and the popular press certainly seems to agree with the notion that some cyberloafing is good for the employee. Specifically, there appears to be a relationship between organizational stressors and cyberloafing, and browsing the Internet can be a palliative way for workers to cope with stress in the workplace (Anandarajan & Simmers, 2005). Occupational stressors that relate to loafing behavior include both role conflict and role ambiguity having a

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

positive relationship with cyberloafing (Blanchard & Henle, 2008). Role conflict exists when demands a worker receives are inconsistent or at odds with each other, and role ambiguity exists when there are unclear job requirements (Rizzo, House, & Lirtzman, 1970). Blanchard and Henle (2008) also found that a negative relationship exists between role overload (i.e. too much to do in too little time) and cyberloafing, such that those who were high in role overload did not cyberloaf as much. Blanchard and Henle's results were supported by Krajcevska, Pindek, and Spector (2017), who found that those experiencing low workload were more apt to cyberloaf, and that the relationship between workload and cyberloafing was possibly mediated by job boredom.

Cyber Incivility

The proliferation of Internet access in the workplace has also allowed for workers to freely communicate with others in an immediate manner through email, and smartphone access has made texting coworkers possible. No longer do you have to wait for the postman or fax machine to send and receive information. Now you can transmit messages rapidly by just typing and hitting "send." Communicating through ICTs has proven invaluable for organizations and their workers. In a study of individuals who have Internet access at work, the Pew Research Center found a large percentage of employees believe email (61%), Internet (54%), and smartphones (24%) are now "very important" to perform their job (Purcell & Rainie, 2014). Though email and texting allow for near instantaneous transmission of communication and for many they are much faster and more efficient to use, tradeoffs exist when using ICTs instead of face-to-face interactions in the workplace. One of the biggest downsides to ICT usage is the loss of important facial expressions, body language and voice inflections that are apparent to others in face-to-face communication. The potential for emails and text messages to be construed as uncivil regardless of intent is likely higher than with in-person communication because of the missing contextual cues and the likelihood that we perceive ourselves to be better at communicating through ICT than we actually are (Kruger, Epley, Parker, & Ng, 2005). Furthermore, the norms regarding appropriate behavior when using ICT are not always as explicit to workers as in face-to-face situations (Park, Fritz, & Jex, 2015).

Cyber incivility refers to rude or uncivil behaviors and comments transmitted through email or text that are interpreted by the recipient as harmful (Giumetti, McKibben, Hatfield, Schroeder, & Kowalski, 2012; Park et al., 2015). As stated earlier in the chapter, the prevalence of workplace incivility is high and the transition to email by most organizations compounds a problem that already frequently occurs. Park et al. (2015) found 36% of workers received at least one email they perceived to be rude each day, while 91% of the respondents in Lim and Teo's (2009) study stated they received uncivil emails from their supervisor. Like workplace incivility, intent to harm is not a necessary requirement of cyber incivility, as many people are unaware that the emails they send appear to

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

others as rude or hostile. Furthermore, some email and texting behaviors that are considered uncivil by recipients are not behaviors that the actor would consider rude or uncivil. Lim and Teo (2009) categorize cyber incivility behaviors into active and passive behaviors, with active behaviors being more directly offensive. Active behaviors include saying hurtful things to others, being condescending, making derogatory remarks, and using email to say negative things that would not be said if in a face-to-face situation. Passive behaviors include using email to schedule or cancel a meeting on short notice, not acknowledging an email was received when acknowledgment is requested, not responding to emails, and using email to communicate when face-to-face communication is considered necessary. Passive email behaviors can be particularly harmful to workers because the recipient often lacks the opportunity to get clarification or feedback from the sender (Lim & Teo, 2009), while also having the ability to ruminate about the email sitting in their inbox (Park et al., 2015).

The effects of cyber incivility behaviors are similar whether they are active or passive in a particular situation, as they both act as a stressor to workers. Consistent with the extant literature on general workplace incivility, the potential negative outcomes of cyber incivility include lower job satisfaction and organizational commitment (Lim & Teo, 2009), higher rates of burnout and withdrawal CWB such as absenteeism and turnover intentions (Giumetti et al., 2012), and an increase in state negative affect (Giumetti et al., 2013). The classification of cyber incivility as a stressor has led to Conservation of Resources (COR) theory being the dominant framework for studying the construct (Giumetti et al., 2013; Giumetti et al., 2012; Park et al., 2015). According to COR theory, resources are “those objects, personal characteristics, conditions, or energies that are valued by the individual” (Hobfoll, 1989, p. 516). People strive to maintain their maximum allotment of resources, and the loss or threat of loss of resources can be a stressor. In a direct test of COR theory as a framework to study cyber incivility, Giumetti et al. (2013) found individuals who interacted with an uncivil supervisor reported lower mental, emotional, and social energy after their interactions, and also had lower task performance than those who interacted with a supportive supervisor through email. Furthermore, participants who interacted with supportive supervisors had higher levels of social energy, resulting in more engagement in their tasks.

In addition to mental and emotional resources, cyber incivility can also affect the physical wellbeing of workers. Individuals who have been the recipient of rude emails throughout a work day are likely to suffer from negative physical symptoms such as headache, upset stomach, and fatigue (Park et al., 2015), impacting both the individual and rising health costs for organizations (Lim & Teo, 2009). The strain that cyber incivility places on workers highlights the need for employees to be able to replenish their resources and be productive and healthy workers. Two resources that Park et al. (2015) found can lower the resource-depleting effects of cyber incivility are job control and psychological detachment from work. Job control refers to the ability for an employee to have autonomy and latitude in how they accomplish their tasks at work (Karasek,

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

1979). Workers high in control of how their tasks were performed showed no relationship between cyber incivility and distress in the workplace, whereas those low in control were affectively and physically distressed at the end of their work day. The ability to psychologically detach from work at home is important for workers to overcome the distress they feel at the end of their work day and be able to replenish their resources for the next day (Park et al., 2015). However, technology has negatively impacted the ability for workers to detach. Receiving emails from supervisors and text messages from coworkers is now commonplace in workers' off-hours, and teleworkers who work from home may also lack the physical detachment from work that those who go to the office experience when they leave work premises. We agree with Park et al. (2015) that those who are subject to cyber incivility during their work day should be cognizant that detachment from work is especially necessary during their off-time immediately following.

Workplace Cyberbullying

As ICT devices and social media platforms became popular, there has been a rise in empirical research studying cyberbullying; however, most of the research in this domain has been conducted with the purpose of studying this phenomenon in adolescents and an educational context (Li, 2006; Smith et al., 2008; Tokunaga, 2010). Perhaps it is unsurprising that the beginnings of cyberbullying research have focused on teenagers and school settings, since nowadays nearly all students are digital natives (i.e. those who have only been alive in the Internet era) and younger generations are quick to adopt the newest social media platforms where much of the cyberbullying activity occurs. The extant literature in this field finds many negative outcomes associated with cyberbullying, including depression, anxiety, trouble sleeping, substance abuse, lower self-esteem, and even suicide (Kowalski, Giumetti, Schroeder, & Lattanner, 2014; Tokunaga, 2010; Vranjes, Baillien, Vandebosch, Erreygers, & De Witte, 2017). Further contributing to making the effects of cyberbullying salient to both researchers and the public is the attention given to the topic by the mainstream media that reported on several cases of young adults being cyberbullied that ended in suicide (nobullying.com, 2017). What might be considered surprising is that the transition to examining the effects of cyberbullying in the workplace has been much slower than its educational counterpart (Vranjes et al., 2017). Workplace cyberbullying can be defined as "a situation over time, an individual is repeatedly subjected to perceived negative acts through technology (e.g., phone, email, web sites, and social media) which are related to their work context" (Farley, Coyne, Axtell, & Sprigg, 2016, p. 295). Similar to workplace bullying that occurs in face-to-face contexts, simply receiving one rude email from a coworker does not constitute cyberbullying, but rather a pattern of harassing behavior targeted toward an individual represents cyberbullying.

The few studies that have examined how widespread the problem of cyberbullying is in organizational settings have used Leymann's (1996) operationalization

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

of bullying (negative behavior directed at an individual at least weekly over a period of at least six months) to study the prevalence of the phenomenon and found between 10 and 18% of employees are targets of workplace cyberbullying (Coyne et al., 2017; Privitera & Campbell, 2009). The negative outcomes individuals suffer from being cyberbullied include higher turnover intentions (Baruch, 2005), and lower psychological wellbeing and job satisfaction (Coyne et al., 2017), with the link between cyberbullying behaviors and job satisfaction being stronger for those bullied in a cyber context than a face-to-face situation. This stronger relationship between cyberbullying and an organizational-related construct is a particularly relevant finding because there are many factors that can contribute to empirical differences between workplace cyberbullying and face-to-face bullying. One of these differentiating factors is the ability for the perpetrator to remain anonymous and invisible to the target (Coyne et al., 2017; Snyman & Loh, 2015). It is probably quite apparent to someone who was going to commit cyberbullying acts that their work email address or mobile phone number used to bully a coworker could be easily tracked by information technology monitoring or examining personnel records. However, actors have many ways to conceal their identity using ICT devices.

In a qualitative study conducted by D'Cruz and Noronha (2013), one participant spoke of someone who used mobile SIM cards to harass her fiancé, also using nonwork computer systems and impersonating others on Facebook to continue their cyberbullying. Another individual (and her colleagues) was subject to bullying on a social networking site by several of her subordinates after they were laid off by their employer. The anonymity that technology provides further complicates matters for those who are bullied by contributing to a feeling of helplessness and an inability to defend themselves because the identity of their attacker can be unknown. Furthermore, the power imbalance (i.e. abusive supervisor bullying a subordinate) that is typical in workplace bullying situations is no longer a prerequisite when the attacker can hide behind a false online persona.

Another factor unique to cyberbullying is the ability for the attacker to humiliate or harass the victim in a public manner that increases the number of people who can witness the acts (Coyne et al., 2017; Snyman & Loh, 2015). For example, an attacker could email large numbers of coworkers simultaneously, or could post harassing words, pictures, or videos to a social networking platform where the public could not only see the harassment, but also comment or participate in the attack on the victim. The wider potential audience of witnesses to bullying tactics can amplify the negative effects on the target, contributing to a theme recurrent in the nascent workplace cyberbullying literature: a feeling of pervasiveness and a lack of boundaries between work and nonwork situations that leads to individuals feeling as there is no escape from the bullying and it is salient in their lives at all times (Coyne et al., 2017; D'Cruz & Noronha, 2013; Snyman & Loh, 2015).

As stated before, the workplace cyberbullying research domain is in its infancy, and while individual and organizational outcomes have recently begun

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

to be explored, the antecedents of workplace cyberbullying are even less researched. Consistent with previous CWB research, Vranjes et al. (2017) propose a theoretical model based on the stressor–strain model and Affective Events Theory (Weiss & Cropanzano, 1996) to understand what leads people to commit cyberbullying behaviors. The Vranjes et al. (2017) model explicates that workplace stressors (e.g., role conflict, interpersonal conflict, organizational climate) lead to emotions such as anger in the perpetrator or fear and sadness in the target, subsequently leading to cyberbullying victimization and perpetration through emotion regulation suppression.

Insider Threat and Cybersecurity Behaviors

The cases of Edward Snowden and Chelsea Manning brought the topic of insider attacks to the forefront of watercooler discussions in the early to mid-2010s. More recent cases such as that of Harold Thomas Martin III, arrested and subsequently indicted for stealing 50 terabytes of electronic data and boxes of paper documents from his employment as a contractor for the US National Security Agency (Chappell, 2017), and those like him are likely to continue the conversation for years to come. But while insider threats may be a more recent target of research for organizational psychologists, they are not a new phenomenon to information security specialists and have been acknowledged as a problem to the safety of an organization's data since the 1980s (Beeler, 1983; Chinchani, Iyer, Ngo, & Upadhyaya, 2005). An insider is anyone who is a current or former employee, contractor, or third party who has access to protected data, networks, and systems of an organization (Nurse et al., 2014), and insider threat can be defined as "an insider's action that puts at risk an organization's data, processes, or resources in a disruptive or unwelcome way" (Pfleeger, Predd, Hunker, & Bulford, 2010, p.170). As organizations regularly keep their data such as intellectual property and personnel records on networked servers, the opportunity for insider threat to occur in today's computerized world is ever-present, and there is a rich body of research devoted to modeling and predicting insider threats (Chinchani et al., 2005; Magklaras & Furnell, 2002; Nurse et al., 2014).

Malicious Insider Threats. Thus far the effort to model insider threat has been assisted by the CWB literature (Axelrad, Sticha, Brdiczka, & Shen, 2013; Greitzer, Kangas, Noonan, & Dalton, 2010; Nurse et al., 2014); however, there are several factors that have acted as hindrances to understanding the process that leads individuals to commit insider attacks. First, there are two distinct categories of attackers who differ in both motive and method of attack: those who are stealing data or committing fraudulent acts (thieves) and those who are attempting to sabotage the organization or specific individuals in the organization (saboteurs). Shaw (2006) found thieves to be motivated by money and greed, yet they were not necessarily technologically adept workers, but rather took advantage of their knowledge of business rules and regulations combined

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

with their network access to steal from within the organization. Saboteurs are often disgruntled employees who are motivated by revenge. This group are often more technologically savvy than thieves and frequently attack the organization through remote access methods such as backdoors. Particularly relevant, saboteurs often appear to be undergoing significant stressful episodes in the workplace, including probation for behavioral issues or even termination. Further complicating the study of insider threat is the fact that most employees who have sufficient access to sabotage or steal from an organization have already gone through pre-employment screening measures and have obtained legitimate access to the organization's data and resources.

The operationalization of insider threat by many security researchers makes it difficult to draw a direct relationship to CWB and its literature. When examining the Pfleeger et al. (2010) definition used above, insider threat refers to "an insider's action," which includes both intentional and unintentional acts. The Pfleeger et al. (2010) definition is not alone in including unintentional acts as a part of insider threat, as this is quite common in insider threat research (e.g., Crossler et al., 2013; Nurse et al., 2014; Warkentin & Willison, 2009). Intentional acts in insider threat include those mentioned above (theft, fraud, sabotage), revenge against the organization or coworkers, and industrial or political espionage (Crossler et al., 2013). These behaviors are sometimes referred to as malicious acts and they are consistent with the operationalization of CWB (e.g., Gruys & Sackett, 2003; Spector et al. 2006) in that they are volitional acts committed against the organization or coworkers.

The personality and emotional predictors of intentional insider acts are similar to those found to be consistent across the CWB domain, including lack of self-control, anger and narcissism (Axelrad et al., 2013; Mehan, 2016). However, Shaw (2006) cautions against focusing solely on personality and trait predictors like these and others such as lack of social skills and self-entitlement. The evaluation and prediction of insider threat requires a more holistic view. The interrelated steps of Shaw's (2006) framework to study the critical factors leading up to an insider attack include the occurrence of a significant occupational or personal stressor in the six months leading up to the attack, negative emotional and behavioral reactions to that occupational stressor that can be exacerbated by personality and trait factors, the reactions being significant enough to draw attention from the organization in the form of formal action (e.g., discipline, counseling), and the formal action being unsuccessful in changing the behavioral direction of the employee. Shaw's (2006) framework is similar to the "hot" affective theories and models often employed in CWB research, such as the Stressor–Emotion model (Spector & Fox, 2005), where environmental factors in the workplace lead to negative emotions, which in turn lead to CWB.

Nonmalicious Insider Threats. Nonmalicious insider threat behaviors are those that unintentionally place an organization's data at risk by being lax in following safe data-handling practices. These can include cyberloafing on

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

external websites using corporate computers, inadvertently posting confidential data onto social media websites, carelessly clicking on spear-phishing emails, forgetting to change passwords, and failing to log off or lock a workstation (Crossler et al., 2013; Warkentin & Willison, 2009). These behaviors most often occur because of human error (i.e., mistakes or accidents), negligence, lack of training, or lack of experience and are the most common type of insider threat (Nurse et al., 2014). That nonmalicious acts are more common than malicious acts, does not mean that the consequences are any less severe. An example that shows the possible magnitude of an attack resulting from nonmalicious insider threat behavior is the April 2015 hack of the Office of Personnel Management (OPM). As a result of the OPM attack, the personnel records of 21.5 million and the fingerprints of 5.6 million individuals were stolen. The hackers were able to obtain access to the data by using social engineering methods to infiltrate and install malware (i.e., malicious software) on OPM's internal network (Koerner, 2016).

Social engineering refers to "use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks" (Abraham & Chengalur-Smith, 2010, p. 183), and the methods used today are much more advanced than a simple email from a Nigerian prince requesting that you send personal information, banking information, or money as quickly as possible. Spear-phishing, a technique where individuals are personally targeted, is increasingly becoming the norm among hackers. It is becoming increasingly more difficult to avoid falling prey to social engineering methods, since much of the information used to bait users comes from publicly available information, especially in today's world where so many individuals have shared personal data on social media websites.

Given this, how can organizations minimize the human component of insider threat by reducing workers' behaviors that cause harm to the organization's data? Regardless of whether the behavior is malicious or unintentional, insider threat and social engineering awareness, training, and education should be mandatory for all employees and available to contractors and third-party vendors that have access to an organization's network. While we have already noted that unintentional acts would not be considered CWBs, that does not mean that the CWB literature cannot be helpful in understanding these behaviors. However, because unintentional insider threat occurs primarily from accidents, negligence, or a lack of training, perhaps the safety literature (e.g., safety training, safety climate, safety interventions) may be a more apt extant literature from which organizational psychologists can assist insider threat researchers. For example, Neal and Griffith (2002) provide evidence that safety climate leads to knowledge and skill motivation, which leads to both safety compliance and safety participation. Adapting this model of safety behaviors to a cybersecurity context could help researchers and organizations by providing a framework that assists companies in their efforts to ensure their employees are more cognizant of the impact their technology-related behavior can have on the organization.

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

Unethical Behavior

Though many of the CWBs and technology-related behaviors mentioned in this chapter would be considered unethical, unethical behavior in the workplace is not limited to CWB. While CWB focuses on behavior that violates organizational norms (Bennett & Robinson, 2000), unethical behavior encompasses behaviors that violate the social and moral norms of the larger community (Kaptein, 2008). Furthermore, CWB harms or is intended to harm the organization or its employees, and there is no such boundary condition regarding unethical behavior. In fact, at times it is quite the opposite. Some unethical behaviors have direct benefits for the organization, and this type of behavior has been referred to as unethical pro-organizational behavior (UPB; Umphress, Bingham, & Mitchell, 2010). Examples of UPB include an employee misrepresenting the truth to make an organization look better, exaggerating the truth to customers about an organization's products or services, and withholding negative information (Umphress et al., 2010). The organization benefiting from UPB aligns the construct more closely with organizational citizenship behavior than with CWB. The unfortunate side of UPB in the workplace is that, though the behaviors may have beneficial effects for the organization, they often can have deleterious effects on employees or prospective employees. Instead of broadly surveying the extant literature of unethical behavior in the workplace, the goal of this section is to examine some of the ethical issues surrounding two UPB domains affected by technology that can have positive outcomes for the organization, while possibly causing negative perceptions in workers or job applicants: workplace monitoring and social media screening/monitoring.

Workplace Monitoring

One obvious tactic that organizations can employ to minimize insider threat and the technology-related CWBs discussed in this chapter is to electronically monitor their employees. But as Dalal and Girab (2016) eloquently state, "just because firms *can* (in terms of technical ability and absence of legal restraints) electronically monitor vast quantities of employee behavior does not mean that they *should* do so without careful forethought" (p. 100). When considering technology-related CWB, electronic monitoring can certainly have positive aspects for both the organization and the worker. In the case of cyber bullying, as long as the perpetrator is not anonymously bullying the target (and sometimes even if they are, their identity can be discovered), there will be an electronic "paper trail" that can provide evidence to help prove to the organization or police that the bullying occurred. Electronic monitoring can be especially helpful for actors and targets of cyber incivility, with emails and responses available to help management deal with conflict and assisting with clarification of misinterpretations that may have occurred between employees when communicating through ICTs. Monitoring workplace Internet traffic has become

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

commonplace (and necessary) as a means to defend the organization against insider threat and can also be used simultaneously to monitor cyberloafing. Twenty years ago, information technology departments could block all outbound Internet traffic to undesired websites and workers were unable to visit nonwork websites during work hours. IT departments can (and do) still do this, but workers can now circumvent this type of monitoring to cyberloaf by using their smartphone, which would require organizations to monitor through other methods such as video monitoring to combat this behavior.

An entire chapter could focus on privacy and legal issues surrounding electronic monitoring, but directly relevant to this chapter is the fact that monitoring affects workers by increasing stress and worsening job attitudes (Alge & Hansen, 2014). As previously mentioned, higher job stress and lower job satisfaction might lead to CWB, and these are the behaviors organizations and organizational psychologists are trying to remedy. The pursuit then becomes how to implement monitoring methods that maximize protection for the organization and employee, while minimizing CWB. A recent study by Glassman, Prosch, and Shao (2015) could offer insight into how to achieve the desired effects. Glassman et al. (2015) developed and examined the effectiveness of an Internet filtering and monitoring tool designed to combat cyberloafing. The tool they designed consisted of three modules: a blocking module, a confirmation module, and a quota module. The blocking module prohibited users from accessing blacklisted websites that were predetermined to be potentially harmful to the organization or counterproductive to work. The confirmation module prompted the user to confirm they were accessing websites for work-related purposes and they were then allowed access for five minutes before receiving another confirmation message. The quota module allowed users to visit nonwork-related websites in ten-minute increments, up to a total of 90 minutes before receiving a message that they had exceeded their daily web usage quota. While all three modules were positively related to appropriate use of Internet resources, the confirmation module was most effective. These findings and the concept of trust and control being important to employees are not new or revolutionary. But, we believe context is important, and the creation of a software program to study browsing habits and the effects of electronic monitoring is an ideal manner in which to research C-CWB.

Social Media Screening/Monitoring

The ubiquitous usage of social media in the past decade has led to increased monitoring of employees by organizations outside the workplace, and even of applicants to organizations. A 2017 CareerBuilder.com study of 2,300 hiring managers and human resource professionals found 70% of employers use social media screening when hiring candidates and 54% have decided to not hire an applicant based on their social media presence (Salm, 2017). Organizations are able to learn through social media screening whether potential employees have posted inappropriate photographs, discriminatory comments, or information

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

about possible drug use or alcohol abuse. However, frequently applicants have negative reactions to organizations screening through social media. In a study design using a realistic hiring scenario, Stoughton, Thompson, and Meade (2015) found those who believed a future employer had used social media screening felt their privacy was invaded, which led to lower organizational attraction (i.e., they were less likely to want to work for that company). In a second study, Stoughton et al. (2015) found those who felt their privacy was invaded also had increased intentions to litigate.

Once employed, a common misconception among employees is that they can't, aren't or shouldn't be regulated by employers (Determann, 2012). However, the aforementioned CareerBuilder.com study reports that approximately half of organizations research current employees' social media presence, and 34% have found content that led to the employee being reprimanded or fired (Salm, 2017). According to the National Labor Relations Board (NLRB), an employee's social media comments are not protected if the employee is complaining about their workplace and the complaints are not in relation to group activity among employees (National Labor Relations Board, 2012). The NLRB also cautions organizations against social media policies that prohibit activity allowed by federal law.

Sometimes though, it is not even the employee's own social media posts that lead to negative consequences. The recent occurrence of identifying individuals on Twitter who took part in the Charlottesville "Unite the Right" rally, subsequently leading to the firing of some individuals from their jobs, supports the notion that sometimes behaviors committed by employees are lawful, yet deemed against societal norms and can lead to organizations terminating them. Off-duty deviance, defined as "behaviors committed by an employee outside the workplace or off-duty that are deviant by organizational and/or societal standards, jeopardize the employee's status within the organization, and threaten the interests and wellbeing of the organization and its stakeholders" (Lyons, Hoffman, Bommer, Kennedy, & Hetrick, 2016, p. 464), is an increasing concern for companies because of the swift nature of information sharing with social media.

It is beyond the scope of this chapter to settle any discussion on the pros and cons of social media monitoring, but we would like to highlight ethical concerns employees and organizations may have as a result of social media usage and monitoring. We would also like to note that the information an employer gleans from intruding into the personal life of its employees may lead to discriminatory practices against the employee and can threaten their privacy, dignity, and freedom (Sánchez Abril, Levin, & Del Riego, 2012), and these threats may lead to negative consequences for both the employee and the organization.

Recommendations for Employers and Organizations

The development of digital technology has created challenges for organizations in managing the behavior that employees engage in and receive

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

from others. The widespread use of the Internet has facilitated many behaviors, both counterproductive and productive. Moving forward we need a better understanding of how technology affects employee behavior, and how we can best minimize detrimental effects. Organization management should develop policies and practices that can provide reasonable monitoring of employee behavior without producing the unintended negative consequences of privacy violation and erosion of trust. In large part this can involve the development of organizational climates that discourage potentially damaging behaviors.

Cyber-mistreatment, such as cyberbullying and cyber incivility, can be approached in much the same way as general bullying and incivility. Organizations should have policies that encourage respectful treatment among employees, and sanction extreme forms of abusive behavior such as bullying. Supervisors should provide support to those targeted, and take corrective actions with those who engage in the behavior. What is important is for there to be trust among supervisors and subordinates so that someone who is a target will feel safe in bringing the issue to his or her supervisor.

Cyberloafing is a complex issue that requires a nuanced response to separate behavior that can be a form of coping that may enhance an individual's ability to properly handle the stresses of a job, versus a withdrawal response by an individual who lacks motivation and is avoiding work. Organizations can develop policies that allow a reasonable amount of cyberloafing as long as it is not detrimental to productivity. One approach is to hold employees accountable for results and not for how they spend their time. Thus, an employee might find that a certain level of pacing is required to avoid excessive fatigue, and that might be accomplished with occasional cyber-breaks.

Insider cybersecurity threat is a complex problem because there are different reasons and mechanisms involved across people. Some cybersecurity should be dealt with as a crime, either theft or purposeful sabotage. Where sensitive data are concerned, systems to monitor access and prevent theft are necessary. Some level of employee monitoring of data is essential to track who accesses data and what is done with it. For nonmalicious threats, the proper handling of data should be considered a vital aspect of job performance, and employees should be held accountable for following proper safety protocols. As noted earlier, there are parallels with the employee accident/safety literature, where success has been achieved with the use of training, and the development of safety climate/culture (Colligan & Cohen, 2004; Wu, Chen, & Li, 2008; Zacharatos, Barling, & Iverson, 2005).

Conclusion

The goal of this chapter was to summarize the research areas of CWB and workplace mistreatment with attention to analogs of newer technology-related behaviors that are becoming more commonplace in today's technology-fueled workplace. We then provided a detailed literature review of

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

newer C-CWB and the C-OHP topics of cyberbullying and cyber incivility. Next, we discussed how workplace monitoring of Internet traffic is becoming a necessity within organizations and social media monitoring is becoming increasingly more commonplace in the hiring, discipline, and firing processes in organizations. Therefore, we highlighted the need for organizations to consider the ethical and wellbeing implications associated with this increased monitoring. While the technology-driven CWB and workplace mistreatment domain is a burgeoning field, we believe the ongoing transition of the workplace (and home) to a technology-fueled world necessitates more attention by organizational psychologists and human resource professionals to these constructs, and we hope this chapter assists with the furthering of technology-related research in this area.

Acknowledgements

Preparation of this chapter was supported by the National Institute of Occupational Safety and Health (NIOSH) and the Sunshine Education and Research Center (Training Grant No. T72OH008438).

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196. https://doi.org/10.1016/j.techsoc.2010.07.001

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11–39). New York, NY: Springer.

Alge, B. J., & Hansen, S. D. (2014). *Workplace monitoring and surveillance research since "1984": A review and agenda*. In M. D. Coovert & L. F. Thompson (Eds.), *The psychology of workplace technology* (pp. 209–237). New York, NY: Routledge/ Taylor & Francis Group.

Anandarajan, M., & Simmers, C. A. (2005). Developing human capital through personal web use in the workplace: Mapping employee perceptions. *Communications of the Association for Information Systems*, *15*(1), 776–791.

Andersson, L. M., & Pearson, C. M. (1999). Tit for tat? The spiraling effect of incivility in the workplace. *The Academy of Management Review, 24*(3), 452–471. doi: 10.2307/259136

Askew, K., Buckner, J. E., Taing, M. U., Ilie, A., Bauer, J. A., & Coovert, M. D. (2014). Explaining cyberloafing: The role of the theory of planned behavior. *Computers in Human Behavior*, *36*, 510–519. doi: 10.1016/j.chb.2014.04.006

Axelrad, E. T., Sticha, P. J., Brdiczka, O., & Shen, J. (2013). *A Bayesian network model for predicting insider threats*. Paper presented at the Security and Privacy Workshops (SPW), 2013 IEEE. San Francisco, CA.

Baruch, Y. (2005). Bullying on the net: Adverse behavior on e-mail and its impact. *Information & Management*, *42*, 361–371. doi: 10.1016/j.im.2004.02.001

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

Beeler, J. (1983). Insiders seen posing greater threat to DP security than outsiders. *Computer World*, *17*(37), 11–12.

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology*, *85*(3), 349–360. doi: 10.1037//0021-9010.85.3.349

Blanchard, A. L., & Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior*, *24*(3), 1067–1084. doi: 10.1016/j.chb.2007.03.008

Challenger, Gray & Christmas (2016). Employers brace for March Madness. Retrieved from www.challengergray.com/press/press-releases/employers-brace-march-madness

Chappell, B. (2017, February 9) Ex-NSA contractor accused of taking classified information is indicted. Retrieved September 7, 2019, from www.npr.org/sections/thetwo-way/2017/02/09/514275544/ex-nsa-contractor-indicted-for-taking-classifed-information

Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005). Towards a theory of insider threat assessment. In *2005 International Conference on Dependable Systems and Networks, Proceedings* (pp. 108–117). Yokohama, Japan.

Colligan, M. J., & Cohen, A. (2004). The role of training in promoting workplace safety and health. In J. Barling, & M. R. Frone (Eds.), *The psychology of workplace safety* (pp. 223–248). Washington, DC: American Psychological Association.

Cortina, L. M., Kabat-Farr, D., Magley, V. J., & Nelson, K. (2017). Researching rudeness: The past, present, and future of the science of incivility. *Journal of Occupational Health Psychology, 22*(3), 299–313. doi: 10.1037/ocp0000089

Cortina, L. M., & Magley, V. J. (2003). Raising voice, risking retaliation: Events following interpersonal mistreatment in the workplace. *Journal of Occupational Health Psychology, 8*(4), 247–265. doi: 10.1037/1076-8998.8.4.247

Coyne, I., Farley, S., Axtell, C., Sprigg, C., Best, L., & Kwok, O. (2017). Understanding the relationship between experiencing workplace cyberbullying, employee mental strain and job satisfaction: A dysempowerment approach. *International Journal of Human Resource Management*, *28*(7), 945–972. doi: 10.1080/09585192.2015.1116454

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. doi: 10.1016/j.cose.2012.09.010

D'Cruz, P., & Noronha, E. (2013). Navigating the extended reach: Target experiences of cyberbullying at work. *Information and Organization*, *23*(4), 324–343. doi: 10.1016/j.infoandorg.2013.09.001

Dalal, R. S., & Girab, A. (2016). Insider threat in cyber security: What the organizational psychology literature on counterproductive work behavior can and cannot (yet) tell us. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), *Psychosocial dynamics of cyber security*: New York, NY: Routledge, 122–140.

Determann, L. (2012). Social media privacy: A dozen myths and facts. *Stanford Technology Law Review*, *7*, 1–14.

Einarsen, S. (2000). Harassment and bullying at work: A review of the Scandinavian approach. *Aggression and Violent Behavior, 5*(4), 379–401. doi: 10.1016/S1359-1789(98)00043-3

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

Einarsen, S., Hoel, H., & Notelaers, G. (2009). Measuring exposure to bullying and harassment at work: Validity, factor structure and psychometric properties of the Negative Acts Questionnaire – revised. *Work and Stress*, *23*(1), 24–44. doi: 10.1080/02678370902815673

Farley, S., Coyne, I., Axtell, C., & Sprigg, C. (2016). Design, development and validation of a workplace cyberbullying measure, the WCM. *Work and Stress*, *30* (4), 293–317. doi: 10.1080/02678373.2016.1255998

Fox, S., & Spector, P. E. (2010). Instrumental counterproductive work behavior and the theory of planned behavior: A "cold cognitive" approach to complement "hot affective" theories of CWB. In L. L. Neider & C. A. Schriesheim (Eds.), *Research in management. The "dark" side of management* (pp. 93–114). Charlotte, NC: IAP Information Age Publishing.

Giumetti, G. W., Hatfield, A. L., Scisco, J. L., Schroeder, A. N., Muth, E. R., & Kowalski, R. M. (2013). What a rude e-mail! Examining the differential effects of incivility versus support on mood, energy, engagement, and performance in an online context. *Journal of Occupational Health Psychology*, *18*(3), 297–309. doi: 10.1037/a0032851

Giumetti, G. W., McKibben, E. S., Hatfield, A. L., Schroeder, A. N., & Kowalski, R. M. (2012). Cyber incivility @ work: The new age of interpersonal deviance. *Cyberpsychology Behavior and Social Networking*, *15*(3), 148–154. doi: 10.1089/cyber.2011.0336

Glassman, J., Prosch, M., & Shao, B. B. M. (2015). To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information & Management*, *52*(2), 170–182. doi: 10.1016/j.im.2014.08.001

Greitzer, F. L., Kangas, L. J., Noonan, C. F., & Dalton, A. C. (2010). *Identifying at-risk employees: A behavioral model for predicting potential insider threats*. Arlington, VA: US Department of Energy,

Gruys, M. L., & Sackett, P. R. (2003). Investigating the dimensionality of counterproductive work behavior. *International Journal of Selection and Assessment, 11*(1), 30–42. doi: 10.1111/1468-2389.00224

Hershcovis, M. S. (2011). "Incivility, social undermining, bullying ... oh my!": A call to reconcile constructs within workplace aggression research. *Journal of Organizational Behavior*, *32*(3), 499–519. doi: 10.1002/job.689

Hobfoll, S. E. (1989). Conservation of resources: A new attempt at conceptualizing stress. *The American Psychologist*, *44*(3), 513–524. http://dx.doi.org/10.1037/0003-066X.44.3.513

Hoel, H., Sheehan, M. J., Cooper, C. L., & Einarsen, S. (2011). Organisational effects of workplace bullying. In S. Einarsen, H. Hoel, D. Zapf, & C. L. Cooper (Eds.), *Bullying and harassment in the workplace: Developments in theory, research, and practice* (pp. 129–148). Boca Raton, FL: CRC Press.

Jex, S. M., & Britt, T. W. (2014). *Organizational psychology: A scientist-practitioner approach* (3rd ed.). Hoboken, NJ: Wiley.

Kaptein, M. (2008). Developing a measure of unethical behavior in the workplace: A stakeholder perspective. *Journal of Management*, *34*(5), 978–1008. doi: 10.1177/0149206308318614

Karasek, R. A., Jr. (1979). Job demands, job decision latitude, and mental strain: Implications for job redesign. *Administrative Science Quarterly*, *24*(2), 285–308. doi: 10.2307/2392498

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

Koerner, B.L. (2016, Oct 23). Inside the cyberattack that shocked the US government. Retrieved September 7, 2019, from www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, *140*(4), 1073–1137. doi: 10.1037/a0035618

Krajcevska, A., Pindek, S., & Spector, P. E. (2017). *Cyberloafing as an adaptive response to boredom*. Paper presented at the Southern Management Association 2017 Conference, Saint Pete Beach, FL.

Krischer, M. M., Penney, L. M., & Hunter, E. M. (2010). Can counterproductive work behaviors be productive? CWB as emotion-focused coping. *Journal of Occupational Health Psychology*, *15*(2), 154–166. doi: 10.1037/a0018349

Kruger, J., Epley, N., Parker, J., & Ng, Z.-W. (2005). Egocentrism over e-mail: can we communicate as well as we think? *Journal of Personality and Social Psychology*, *89*(6), 925–936. doi: 10.1037/0022-3514.89.6.925

Leymann, H. (1996). The content and development of mobbing at work. *European Journal of Work and Organizational Psychology, 5*(2), 165–184. doi: 10.1080/13594329608414853

Li, Q. (2006). Cyberbullying in schools: A research of gender differences. *School Psychology International*, *27*(2), 157–170. doi: 10.1177/0143034306064547

Liberman, B., Seidman, G., McKenna, K. V. A., & Buffardi, L. E. (2011). Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Computers in Human Behavior*, *27*(6), 2192–2199. doi: 10.1016/j.chb.2011.06.015

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, *23*(5), 675–694. doi: 10.1002/job.161

Lim, V. K. G., & Chen, D. J. Q. (2012). Cyberloafing at the workplace: Gain or drain on work? *Behaviour & Information Technology, 31*(4), 343–353. doi: 10.1080/01449290903353054

Lim, V. K. G., & Teo, T. S. H. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore – An exploratory study. *Information & Management*, *42*(8), 1081–1093. doi: 10.1016/j.im.2004.12.002

Lim, V. K. G., & Teo, T. S. H. (2009). Mind your E-manners: Impact of cyber incivility on employees' work attitude and behavior. *Information & Management*, *46*(8), 419–425. doi: 10.1016/j.im.2009.06.006

Lyons, B. D., Hoffman, B. J., Bommer, W. H., Kennedy, C. L., & Hetrick, A. L. (2016). Off-duty deviance: Organizational policies and evidence for two prevention strategies. *Journal of Applied Psychology*, *101*(4), 463–483.

Magklaras, G. B., & Furnell, S. M. (2002). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62–73.

Mehan, J. E. (2016). *Insider threat: A guide to understanding, detecting, and defending against the enemy from within*: Ely, UK: IT Governance Publishing.

National Labor Relations Board (2012). The NLRB and social media. Retrieved September 9, 2019, from www.nlrb.gov/rights-we-protect/rights/nlrb-and-social-media

Neal, A., & Griffith, M. A. (2002). Safety climate and safety behaviour. *Australian Journal of Management*, *27*(Special Issue), 67–75.

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

Niedl, K. (1996). Mobbing and well-being: Economic and personnel development implications. *European Journal of Work and Organizational Psychology*, *5*(2), 239–249. doi: 10.1080/13594329608414857

nobullying.com. (2017). The top six unforgettable cyberbullying cases ever. Retrieved September 7, 2019, from https://nobullying.com/six-unforgettable-cyber-bullying-cases/

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). *Understanding insider threat: A framework for characterising attacks*. Paper presented at the Security and Privacy Workshops (SPW), 2014 IEEE. San Jose, CA.

O'Neill, T. A., Hambley, L. A., & Bercovich, A. (2014). Prediction of cyberslacking when employees are working away from the office. *Computers in Human Behavior*, *34*, 291–298. doi: 10.1016/j.chb.2014.02.015

Park, Y., Fritz, C., & Jex, S. M. (2015). Daily cyber incivility and distress: The moderating roles of resources at work and home. *Journal of Management*. doi: 10.1177/0149206315576796

Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security*, *5*(1), 169–179. doi: 10.1109/TIFS.2009.2039591

Porath, C., & Pearson, C. (2013). The price of incivility. *Harvard Business Review, 91*(1/2), 114–121.

Privitera, C., & Campbell, M. A. (2009). Cyberbullying: The new face of workplace bullying? *Cyberpsychology & Behavior*, *12*(4), 395–400. doi: 10.1089/cpb.2009.0025

Purcell, K., & Rainie, L. (2014). Technology's impact on workers. Retrieved from www.pewinternet.org/2014/12/30/technologys-impact-on-workers/

Restubog, S. L. D., Garcia, P., Toledano, L. S., Amarnani, R. K., Tolentino, L. R., & Tang, R. L. (2011). Yielding to (cyber)-temptation: Exploring the buffering role of self-control in the relationship between organizational justice and cyberloafing behavior in the workplace. *Journal of Research in Personality*, *45*(2), 247–251. doi: 10.1016/j.jrp.2011.01.006

Rizzo, J. R., House, R. J., & Lirtzman, S. I. (1970). Role conflict and ambiguity in complex organizations. *Administrative Science Quarterly*, *15*(2), 150–163.

Salm, L. (2017). 70% of employers are snooping candidates' social media profiles. Retrieved from www.careerbuilder.com/advice/social-media-survey-2017

Sánchez Abril, P., Levin, A., & Del Riego, A. (2012). Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal*, *49*(1), 63–124. doi: 10.1111/j.1744-1714.2011.01127.x

Schilpzand, P., de Pater, I. E., & Erez, A. (2016). Workplace incivility: A review of the literature and agenda for future research. *Journal of Organizational Behavior*, *37*, S57–S88. doi: 10.1002/job.1976

Shaw, E. D. (2006). The role of behavioral research and profiling in malicious cyber insider investigations. *Digital Investigation*, *3*(1), 20–31. https://doi.org/10.1016/j.diin.2006.01.006

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376–385. doi: 10.1111/j.1469-7610.2007.01846.x

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

Snyman, R., & Loh, J. M. I. (2015). Cyberbullying at work: The mediating role of optimism between cyberbullying and job outcomes. *Computers in Human Behavior*, *53*, 161–168. doi: 10.1016/j.chb.2015.06.050

Spector, P. E., & Fox, S. (2005). The stressor–emotion model of counterproductive work behavior. In S. Fox, & P. E. Spector (Eds.), *Counterproductive work behavior: Investigations of actors and targets.* (pp. 151–174). Washington, DC: American Psychological Association.

Spector, P. E., Fox, S., Penney, L. M., Bruursema, K., Goh, A., & Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviors created equal? *Journal of Vocational Behavior, 68*(3), 446–460. doi: 10.1016/j.jvb.2005.10.005

Stoughton, J. W., Thompson, L. F., & Meade, A. W. (2015). Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Business and Psychology*, *30*(1), 73–88. doi: 10.1007/s10869-013-9333-6

Tepper, B. J. (2000). Consequences of abusive supervision. *Academy of Management Journal, 43*(2), 178–190. doi: 10.2307/1556375

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, *26*(3), 277–287. doi: 10.1016/j.chb.2009.11.014

Umphress, E. E., Bingham, J. B., & Mitchell, M. S. (2010). Unethical behavior in the name of the company: The moderating effect of organizational identification and positive reciprocity beliefs on unethical pro-organizational behavior. *Journal of Applied Psychology*, *95*(4), 769–780. doi: 10.1037/a0019214

Van den Brande, W., Baillien, E., De Witte, H., Vander Elst, T., & Godderis, L. (2016). The role of work stressors, coping strategies and coping resources in the process of workplace bullying: A systematic review and development of a comprehensive model. *Aggression and Violent Behavior*, *29*, 61–71. doi: 10.1016/j.avb.2016.06.004

Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2017). The dark side of working online: Towards a definition and an Emotion Reaction model of workplace cyberbullying. *Computers in Human Behavior*, *69*, 324–334. doi: 10.1016/j.chb.2016.12.055

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105. doi: 10.1057/ejis.2009.12

Weiss, H. M., & Cropanzano, R. (1996). Affective events theory: A theoretical discussion of the structure, causes and consequences of affective experiences at work. *Research in Organizational Behavior*, *18*, 1–74.

Wu, T. C., Chen, C. H., & Li, C. C. (2008). A correlation among safety leadership, safety climate and safety performance. *Journal of Loss Prevention in the Process Industries*, *21*(3), 307–318. https://doi.org/10.1016/j.jlp.2007.11.001

Yang, L. Q., Caughlin, D. E., Gazica, M. W., Truxillo, D. M., & Spector, P. E. (2014). Workplace mistreatment climate and potential employee and organizational outcomes: A meta-analytic review from the target's perspective. *Journal of Occupational Health Psychology*, *19*(3), 315–335. doi: 10.1037/a0036905

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press

Zacharatos, A., Barling, J., & Iverson, R. D. (2005). High-performance work systems and occupational safety. *Journal of Applied Psychology*, *90*(1), 77–93. doi: 10.1037/0021-9010.90.1.77

Zakrzewski, C. (2016). The key to getting workers to stop wasting time online. Retrieved from www.wsj.com/articles/the-key-to-getting-workers-to-stop-wasting-time-online-1457921545

https://doi.org/10.1017/9781108278034.024 Published online by Cambridge University Press