Knowledge sabotage as an extreme form of counterproductive knowledge behavior: conceptualization, typology, and empirical demonstration

Alexander Serenko

Alexander Serenko is based at the Faculty of Information, University of Toronto, Toronto, Canada.

Abstract

Purpose – *This paper introduces the concept of knowledge sabotage as an extreme form of counterproductive knowledge behavior, presents its typology, and empirically demonstrates its existence in the contemporary organization.*

Design/methodology/approach – *Through the application of the critical incident technique, this study analyzes 177 knowledge sabotage incidents when employees intentionally provided others with wrong knowledge or deliberately concealed critical knowledge while clearly realizing others' need for this knowledge and others' ability to apply it to important work-related tasks.*

Findings – *Over 40% of employees engaged in knowledge sabotage, and many did so repeatedly. Knowledge saboteurs usually acted against their fellow co-workers, and one-half of all incidents were caused by interpersonal issues resulting from the target's hostile behavior, failure to provide assistance to others, and poor performance. Knowledge sabotage was often expressed in the form of revenge against a particular individual, who, as a result, may have been reprimanded, humiliated or terminated. Knowledge saboteurs rarely regretted their behavior, which further confirmed the maliciousness of their intentions.*

Practical implications – *Even though knowledge saboteurs only rarely acted against their organizations purposely, approximately one-half of all incidents produced negative, unintentional consequences to their organizations, such as time waste, failed or delayed projects, lost clients, unnecessary expenses, hiring costs, products being out-of-stock, understaffing, or poor quality of products or services. Organizations should develop comprehensive knowledge sabotage prevention policies. The best way to reduce knowledge sabotage is to improve inter-personal relationships among employees and to foster a friendly and collaborative environment.*

Originality/value – *This is the first well-documented attempt to understand the phenomenon of knowledge sabotage.*

Keywords *Knowledge sharing, Critical incident technique, Counterproductive workplace behaviour, Knowledge sabotage*

Paper type *Research paper*

1. Introduction

As businesses become more knowledge-dependent, the optimization of intra-organizational knowledge flows has turned into a strategic priority for a successful contemporary organization. Efficient knowledge management practices, particularly inter-employee knowledge sharing, have been shown to have a strong positive effect on organizational competitiveness, innovativeness and performance (Andreeva and Kianto, 2012; Kianto *et al.*, 2013; Donate and Guadamillas, 2015; Lin, 2015; Yahyapour *et al.*, 2015; Buenechea-Elberdin *et al.*, 2018). It is for this reason, there is a growing volume of

Received 3 January 2018
Revised 30 June 2018
2 January 2019
Accepted 15 April 2019

research pertaining to various knowledge sharing practices, and knowledge sharing has become the second most frequently used keyword in academic publications (Gaviria-Marin *et al.*, 2018). At the same time, evidence suggests that employees often engage in counterproductive knowledge behavior, such as disengagement from knowledge sharing (Ford *et al.*, 2015), knowledge sharing ignorance (Israilidis *et al.*, 2015), partial knowledge sharing (Ford and Staples, 2010), knowledge hoarding (Hislop, 2003), counter-knowledge sharing (Cegarra-Navarro *et al.*, 2015; Martelo-Landroguez *et al.*, 2019) and knowledge hiding (Connelly *et al.*, 2012; Rhee and Choi, 2017; Jha and Varkkey, 2018; Pan *et al.*, 2018). The present study extends this line of inquiry by introducing a novel concept, referred to as *knowledge sabotage*, which is the most extreme form of counterproductive knowledge behavior.

The notion of workplace sabotage is as old as management literature itself (Taylor, 1911; Williams, 1921; Mathewson, 1931). Saboteurs generally act against their organizations, customers or employees by subverting organizational processes or harming others while, at the same time, pursuing their personal, ego-driven goals (Crino, 1994). The present study proposes and empirically demonstrates that employees may also sabotage organizational knowledge processes by intentionally providing others with wrong knowledge or deliberately concealing critical knowledge while clearly realizing others' need for this knowledge and others' ability to apply it to important work-related activities. Similar to other types of workplace sabotage, knowledge saboteurs may act against their organization or a particular individual (e.g. a manager, a colleague, a subordinate) by focusing on their personal goals and realizing, at least to some extent, the consequences of their action. Knowledge saboteurs may react to someone's request (e.g. provide a wrong document in response to a colleague's inquiry) or initiate the act of sabotage themselves (e.g. voluntarily approach a colleague and deliberately offer wrong advice).

Managers tend to ignore incidents of workplace sabotage in the hope that these are one-time, exceptional events that will eventually fade away (Analoui, 1995). Indeed, identifying, documenting, and labeling an incident as an act of sabotage rather than as an honest mistake requires elaborate organizational policies, legal expertise and moral courage. However, given the exponentially increasing value of knowledge in the contemporary workplace, the application of wrong knowledge or the inability to apply proper knowledge may have devastating consequences for the contemporary organization. As the present study reveals, the negative impacts of even presumably trivial incidents of knowledge sabotage may be more far-reaching than anyone initially envisioned. For example, knowledge sabotage victims often get reprimanded, humiliated or embarrassed which makes them leave their organization. They waste time re-doing important tasks, reduce their productivity or fail entire projects. As a result, their organizations lose human capital, waste financial resources, become less efficient, and reduce the quality of products and services. Because such outcomes contradict the very purpose of successful management practices, it behooves managers to become aware of the existence of knowledge sabotage to reduce or completely eliminate such harmful behavior of their employees.

The purpose of this study is to explore and document the existence of knowledge sabotage as a form of counterproductive knowledge behavior. First, this study develops a conceptual definition of the phenomenon and its key characteristics. Second, it proposes a typology of knowledge sabotage where incidents are mapped within a two-by-two matrix. Third, it empirically demonstrates the existence of knowledge sabotage and validates the proposed typology through the application of the Critical Incident Technique to solicit 177 knowledge sabotage incidents which were analyzed along several dimensions. Based on the findings, this study provides a number of theoretical and practical insights.

2. Literature review

2.1 Workplace sabotage

Counterproductive workplace behavior represents "volitional acts that harm or intend to harm organizations and their stakeholders" (Spector and Fox, 2005, p. 151). They may be targeted at the organization or aimed at an individual – for example, a manager, a co-worker or a subordinate (Robinson and Bennett, 1995). Examples directed towards an organization include theft (Greenberg, 1990), property destruction (Crino, 1994), brand damage (Wallace and de Chernatony, 2008), time and resources wastage, leaking sensitive information to the third parties, non-compliance with service standards, product tempering, tardiness, absenteeism (Robinson and Bennett, 1995), engagement in unsanctioned activities during work hours (Brock *et al.*, 2013), and cyberloafing (Ugrin and Pearson, 2013). Common incidents against an individual are bullying (Harvey *et al.*, 2009; Bartlett and Bartlett, 2011), aggression (Neuman and Baron, 2005), violence (LeBlanc and Barling, 2005), incivility (Pearson *et al.*, 2005) and emotional abuse (Keashly and Harvey, 2005). This negative behavior is triggered by three factors:

1. organizational and work-related issues – poor organizational culture and deviant norms (Bennett *et al.*, 2005; Pilch and Turska, 2015), organizational constraints (Meier and Spector, 2013), unrealistic supervisory demands (Spector and Fox, 2010b), job dissatisfaction (Dalal, 2005; Zhang and Deng, 2016), injustice (Ambrose *et al.*, 2002), customer-related stressors (Wang *et al.*, 2011; Kao *et al.*, 2014);

2. interpersonal issues – colleagues' poor performance (Spector and Fox, 2010a), interpersonal conflict (Andersson and Pearson, 1999); and

3. personal concerns – cynicism towards the top management (Abubakar and Arasl, 2016), emotional dissonance and burnout (Lee and Ok, 2014), the fear of change (Harris, 2002), boredom (Bruursema *et al.*, 2011), various personality traits (Giacalone and Knouse, 1990), such as anxiety, anger, locus of control issues, psychopathy, Machiavellianism and narcissism (Spector and Fox, 2005; Boddy, 2011; Cohen, 2016).

The resulting behavior, in turn, has a negative impact on organizational costs, productivity, reputation and culture as well as on the physical and emotional health and motivation of employees (Bartlett and Bartlett, 2011; Boddy, 2014).

At the same time, counterproductive workplace behavior is a very general concept. It is "considered an umbrella term that subsumes, in part or whole, similar constructs concerning harmful behaviors at work" (Spector and Fox, 2010b, p. 133). Workplace sabotage is a category of counterproductive workplace behavior (Klotz and Buckley, 2013) defined as the employees' actions with the intention "to damage, disrupt or subvert the organization's operations for the personal purposes of the saboteur [...] or the harming of employees or customers" (Crino, 1994, p. 312). Workplace sabotage is a conscious, goal-oriented behavior, and the incidents "constitute deliberate interference with normal company activities and relationships, and each [episode] is characterized by prior thought and appreciation of likely consequences" (Crino, 1994, p. 312).

Workplace sabotage has long been well-documented in various forms and contexts (Klotz and Buckley, 2013). For example, in 1519, during his voyage to circumvent the globe, Ferdinand Magellan had to deal with a mutiny organized by his disgruntled captains who sabotaged the mission of their expedition (Butterworth, 2017). Eventually, mutiny became a well-organized strategy to sabotage the power of legitimate authority as a response to perceived injustice (Coye *et al.*, 2010). As well, the uprisings of machine-destroyers referred to as "The Luddites" who objected to the mechanization of production during the Industrial Revolution turned into one of the largest sabotage movements of the nineteenth century (Jones, 2013). The phenomenon of workplace sabotage was also described by Taylor (1911) over a century ago in his *Principles of Scientific Management*, when he observed that employees tend to work at

the pace of the slowest of them even though this practice contradicts their own self-interest. Williams (1921) and Mathewson (1931) further acknowledged the existence of sabotage in the form of the restriction of output and production pace by informal worker groups, and similar findings were reported in the classical Hawthorne studies (Roethlisberger and Dickson, 1956; Muldoon, 2012). By the end of the twentieth century, various organizational stakeholder groups realized the magnitude and impact of the issue, and scholars embarked on a systematic inquiry into the nature, antecedents and consequences of workplace sabotage (Klotz and Buckley, 2013). Several researchers also mentioned that it is possible to sabotage organizational knowledge processes (Henrie and Hedgepeth, 2003; Hari *et al.*, 2005; Gameson *et al.*, 2008; Serenko and Bontis, 2016), yet, to the best knowledge of the author, no conceptual or empirical work has been done to understand the phenomenon of knowledge sabotage.

2.2 Knowledge sabotage

2.2.1 Conceptualization. Intra-organizational knowledge sharing – defined as an activity in which employees voluntarily share their tacit (i.e. expertise, skills, know-how, know-who, know-where) and explicit (i.e. reports, templates, documents, videos) knowledge with their co-workers (Nonaka, 1994; Bock *et al.*, 2005) – has traditionally been one of the most important research topics within the knowledge management discipline because it has a tremendous impact on organizational performance (Heisig *et al.*, 2016). For example, there are estimates that Fortune 500 companies lose a combined $31.5 billion per year because of their employees' inability to effectively share their knowledge (Myers, 2015). When knowledge is not shared, employees duplicate each others' work, repeat mistakes that have already been made, waste time searching for information when others already know it, fail to locate internal experts, cannot accumulate and re-use best practices, and lose expertise as a result of attrition – all of which reduces productivity and increases organizational costs. For this reason, many researchers have attempted to understand knowledge sharing barriers (Riege, 2005; Ardichvili *et al.*, 2006; Bundred, 2006; Paulin and Suneson, 2012), and the study of counterproductive knowledge behavior has become a leading topic in knowledge management research (Lin and Huang, 2010; Tsay *et al.*, 2014; Wang *et al.*, 2014; Kang, 2016; Bogilović, Černe and Škerlavaj, 2017; Černe *et al.*, 2017; de Geofroy and Evans, 2017; Fang, 2017; Trusson *et al.*, 2017; Fong *et al.*, 2018; Malik *et al.*, 2018; Hernaus *et al.*, 2019).

The extant literature presents several types of counterproductive knowledge behaviors – disengagement from knowledge sharing, knowledge sharing ignorance, partial knowledge sharing, knowledge hoarding, counter-knowledge sharing, and knowledge hiding – which differ in terms of their negative impact on an organization. *Disengagement from knowledge sharing* takes place when employees do not actively communicate their knowledge to their co-workers, even though they have no motivation to hide it (Ford *et al.*, 2015). This happens because employees are so busy with their current tasks that they have no time or resources to help others. Some of them may be also completely disengaged from their organization and solely focus on the tasks they are required to complete to merely keep their job. In this case, there is no malicious intent, and negative consequences are very minor. *Knowledge sharing ignorance* is an "inability that prevents employees from effectively managing the knowledge possessed by organizations" (Israilidis *et al.*, 2015, p. 1113). It refers to the employees' failure to recognize the knowledge they possess, which prevents them from offering it to their colleagues. Ignorant individuals also cannot identify the intellectual capital already existing within their organization, which precludes them from searching for intra-organizational knowledge to improve their effectiveness and efficiency. In other words, ignorant employees do not know what they and the other organizational members know, and they are fully content with this situation. Nevertheless, ignorant knowledge sharing behavior carries little malicious intent, and its negative impact is small.

Partial knowledge sharing refers to incidents when employees share only some of the relevant knowledge with their co-workers (i.e. full knowledge is not disclosed) because they believe that their knowledge is highly valuable and unique, or they distrust the knowledge recipient (Ford and Staples, 2010). In such situations, those who share only partial knowledge have some ego-driven, counterproductive motives in mind, and knowledge recipients may not take full advantage of the knowledge possessed by the donors, which, in turn, negatively impacts their organizations. *Knowledge hoarding* is the deliberate accumulation of knowledge by employees while concealing the fact that they possess this knowledge (Hislop, 2003; Lee *et al.*, 2011; Evans *et al.*, 2015; Holten *et al.*, 2016; Zhao and Xia, 2017). On the one hand, knowledge hoarders develop a tremendous degree of expertise and become highly efficient at their job. On the other hand, knowledge hoarding does not allow organizations to realize the full potential of the intellectual capital possessed by their individual members since the hoarders' knowledge is not shared with others. Knowledge hoarders are generally motivated by their personal interests and the desire to perceive themselves as the only true experts in their organizations – at the expense of the overall organizational performance. *Counter-knowledge sharing* refers to the spread of disinformation and misconceptions coming from unverified sources, such as rumors, gossips, hoaxes, and exaggerations (Cegarra-Navarro *et al.*, 2015; Martelo-Landroguez *et al.*, 2019). However, this behavior results from ignorance and misunderstanding rather than from direct malicious intentions. *Knowledge hiding* refers to the intentional attempts of employees to conceal their knowledge when their fellow colleagues request it (Connelly *et al.*, 2012; Černe *et al.*, 2014; Connelly and Zweig, 2015; Huo *et al.*, 2016; Škerlavaj *et al.*, 2018). In such situations, knowledge owners receive an unambiguous request to share their knowledge, but they make a conscious decision not to disclose what they know. Compared to the counterproductive knowledge behaviors discussed above, knowledge hiding has the most negative impact on organizations.

The present study goes a step further and argues that employees may also engage in knowledge sabotage, which is the most extreme form of counterproductive knowledge behavior in terms of its malicious intent and its negative consequences. *Knowledge sabotage* is defined as an incident when an employee (i.e. the saboteur) provides incorrect (i.e. wrong) knowledge to another employee (the target) or conceals knowledge from another employee under the following conditions:

- the saboteur acts intentionally (intention);
- the saboteur is fully aware of the target's need for knowledge (need awareness);
- the saboteur possesses the required knowledge (knowledge possession);
- the required knowledge is extremely important to the target (knowledge importance);
- the saboteur is aware of the knowledge's importance to the target (knowledge importance awareness); and
- the saboteur is aware that the target would be able to productively apply the required knowledge to work-related tasks (knowledge application).

None of the other counterproductive knowledge behaviors meets all of the criteria above (see Table I). Employees engaged in knowledge hiding possess the required knowledge, are aware of the target's need for knowledge, and act deliberately (Connelly *et al.*, 2012). At the same time, they do not know whether this knowledge is of critical importance and whether the requester will be able to productively apply it to his or her work. For example, an employee may ignore a co-worker's request for a document because he/she may assume that it is not fully relevant to the requester's job or that the requester would be able to quickly locate it her/himself if needed. In contrast, employees engaged in knowledge sabotage may intentionally provide the requester with a wrong document or conceal the correct one while realizing the document's importance and the requester's inability to

Table I Counterproductive knowledge behaviors

	Disengagement from knowledge sharing	*Knowledge sharing ignorance*	*Partial knowledge sharing*	*Knowledge hoarding*	*Counter-knowledge sharing*	*Knowledge hiding*	*Knowledge sabotage*
Intention	No	No	Yes	Yes	No	Yes	Yes
Need awareness	No	No	No	No	No	Yes	Yes
Knowledge possession	No	No	Yes	Yes	No	Yes	Yes
Knowledge importance	No	No	No	No	No	No	Yes
Knowledge importance awareness	No	No	No	No	No	No	Yes
Knowledge application	No	No	No	No	No	No	Yes
Negative impact on an organization	Small	Small	Medium	Medium	Strong	Strong	Very strong

correctly, effectively, and efficiently complete the job-related task without it. Employees engaging in knowledge hoarding and partial knowledge sharing may not even realize the co-worker's need for knowledge and may simply pursue their personal self-interest to accumulate and retain knowledge while not trying to act against someone. Knowledge saboteurs, however, intentionally act against their organization and/or another individual.

2.2.2 Typology. Table II presents the typology of knowledge sabotage behavior. It shows that knowledge sabotage behavior may be classified based on the provoked vs unprovoked dimension. The provoked type assumes the presence of a formal or informal request for knowledge – for example, an email from a supervisor or a verbal inquiry from a colleague. The unprovoked type posits the absence of a knowledge request in any form; nevertheless, the saboteur becomes aware of the target's need for knowledge. For example, one may overhear a conversation or realize a need based on a colleague's behavior or the nature of activities. The saboteur is not approached for important knowledge, yet, upon realizing a need, he/she willingly decides to provide incorrect knowledge or withhold correct knowledge from the target.

Buss (1961) suggests that counterproductive workplace behavior may be categorized along the active-passive dichotomy: active (when the saboteur directly interacts with the target while trying to cause harm) and passive (when the saboteur does not directly interact with the target, avoids interaction, or acts behind one's back while trying to cause harm). Examples of active behavior include assault, hostile actions, obscene gestures, threats and negative comments. Instances of passive behavior include exclusion from important work-related activities and social gatherings, prevention from self-expression, the silent treatment and showing little sympathy during difficult times. Most importantly, passive counterproductive workplace behavior also includes refusing to provide the necessary resources, ignoring the target's requests, and failing to transmit information (Neuman and Baron, 2005). Analoui (1995, p. 56) concludes that passive sabotage takes place when "as a result of deliberate inaction predictable destruction occurred", and a recent employee

Table II Knowledge sabotage typology

		Dimension	
		Active (provides wrong knowledge)	*Passive (conceals knowledge)*
Dimension	Provoked (formal knowledge request)	Provoked-active (provides wrong knowledge upon request)	Provoked-passive (conceals knowledge upon request)
	Unprovoked (no formal knowledge request)	Unprovoked-active (provides wrong knowledge without request)	Unprovoked-passive (conceals knowledge without request)

survey by DecisionWise shows that around 28 per cent of workers have engaged in passive workplace sabotage (Maylett, 2017). With respect to knowledge sabotage, it is reasonable to assume that employees may engage in active sabotage by deliberately providing the target with incorrect critical knowledge or in passive sabotage by ignoring the target's need for critical knowledge.

As such, the literature emphasizes the presence of counterproductive knowledge behavior in the contemporary organization. At the same time, none of the previous studies have approached the phenomenon from the sabotage perspective – when the perpetrator deliberately engages in an extreme form of counterproductive knowledge behavior which may lead to detrimental consequences for the entire organization and/or its employees. The present investigation attempts to fill that void by exploring knowledge sabotage in organizational settings and empirically demonstrating its existence.

3. Methodology

The present study employs the Critical Incident Technique (CIT) (Flanagan, 1954). The CIT is a flexible set of guidelines for collecting important facts regarding human behavior in particular situations to solve practical problems and develop theoretical principles (Butterfield *et al.*, 2005). It is founded on the assumption that individuals may recall highly important incidents and accurately describe them in self-reports. An incident is "any observable human activity that is sufficiently complete in itself to permit inferences and predictions to be made about the person performing the act" (Flanagan, 1954, p. 327). Researchers generally ask the participants to provide brief factual reports of their behavior, a rationale for their action, and the consequences of their behavior. The sample size depends on the complexity of the phenomenon under investigation: a majority of studies collect and analyze from 50 to 100 critical incidents (Urquhart *et al.*, 2003).

As a data collection method, the CIT was selected for the following reasons. *First*, the goal was to document the potential existence of knowledge sabotage incidents. Knowledge sabotage events represent an extreme form of counterproductive human behavior in organizations and, therefore, are likely to be accompanied by strong emotions. According to psychology research, events associated with extreme emotions are likely to be retained in one's long-term memory (LaBar and Cabeza, 2006). Prior research shows that the CIT may serve as a fruitful approach to solicit such memorable episodes associated with negative emotions (Stach and Serenko, 2009; Serenko and Turel, 2010). *Second*, knowledge sabotage represents a category of unethical behavior, and the CIT can be successfully applied in this domain. In the field of ethics, the first documented attempt to employ the CIT dates back to 1948 when the American Psychological Association developed ethical standards for its members (Hobbs, 1948). Since then, the CIT has become a well-established technique in business research focusing on questionable employee actions (McNeil and Pedigo, 2001; Byrne *et al.*, 2014). The application of the CIT allows researchers to collect instances of questionable and unethical behavior and group them into clusters (Small and Cullen, 1995). *Third*, the application of the CIT may help researchers successfully develop new frameworks and taxonomies (Lee *et al.*, 2003; Serenko, 2006), which is aligned with the goal of the present study – to create and empirically validate a typology of knowledge sabotage. *Fourth*, the CIT is also suitable for the collection of self-administered surveys containing open-ended questions (Wang *et al.*, 2000), which fits the context of the present study.

Four brief scenarios (i.e. Provoked-Active, Unprovoked-Active, Provoked-Passive, Unprovoked-Passive) were developed based on the definition of knowledge sabotage, and each clearly mentioned intention, need awareness, knowledge possession, knowledge importance, knowledge importance awareness, and knowledge application (Appendix). These scenarios were subjected to extensive face-validity assessment involving a group of ten academics and practitioners, and adjustments to the instrument were made after three rounds

of revisions. The research method relied on qualitative methodology due to a nascent nature of the phenomenon of interest. At this stage, it was impossible to develop a model explicating a knowledge sabotage process, its antecedents, and its consequences because of a lack of empirical evidence and a theoretical base describing the focal constructs.

Two versions of the instrument were developed: pre-screening and full study. In the pre-screening version, respondents were presented with the four scenarios, each of which was accompanied by a single question: "During your entire working career, how many times have you experienced a situation similar to the one described above?" Answer options ranged from "never" to "over 20". The scenarios in the full-study version were accompanied by five questions: incident description; the target; motivation; impact; and regret. These questions were designed to fully comprehend the situation, the saboteur's actions, the rationale, and the impact on the organization and/or others. To avoid order bias, multiple versions of the instruments (for both the pre-screening and full-study versions) were developed in which the situations were presented in different sequences. The instrument also contained basic demographic questions. The instructions described the study as a neutral "knowledge sharing project," and the word "sabotage" was never mentioned to avoid bias.

Respondents were recruited from the Amazon's Mechanical Turk (mTurk), which is an online marketplace for work that requires human intelligence. mTurk was selected for the following reasons. *First*, knowledge sabotage represents unprofessional conduct which is generally perceived highly negatively, and, therefore, documenting it requires the assurance of complete anonymity of the source to eliminate social desirability bias (Crowne and Marlowe, 1960). mTurk guarantees respondents' anonymity because the researcher may only see their mTurk Worker ID (i.e. no personal information is provided). As a result, the respondents are unlikely to exhibit bias in their responses and report their true opinions, perceptions and facts. *Second*, mTurk allows researchers to pre-screen the respondents by establishing various participation qualifications. *Third*, mTurk participants are more geographically diverse than standard internet and university student samples (Buhrmester *et al.*, 2011), which increases results generalizability.

Only individuals who had at least two years of full-time work experience and were US residents were allowed to participate in the study. Data collection proceeded in two phases. In phase one, the pre-screening instrument was posted on mTurk, and the participants were offered a small compensation (US$0.05). Three hundred and forty-two individuals completed the pre-screening instrument. Out of them, 145 (42 per cent) engaged in at least one of the four types of knowledge sabotage, and they were invited to participate in the second phase to complete the full version of the instrument for a larger compensation (US$3.00). One hundred of them completed the full instrument, at the response rate of 69 per cent.

Several proactive measures were taken to ensure data validity. *First*, only reliable mTurk participants (i.e. workers) were recruited. For this, the following worker requirements were established on mTurk (i.e. only those who met these requirements were able to see and enroll in the survey): HIT (Human Intelligence Task) approval rate = 96 per cent (i.e. the participant had to successfully complete at least 96 per cent of the previous tasks); location = USA; and the number of HITs approved = 1,000 (i.e. the participant had to successfully complete at least 1,000 previous tasks). This was done to ensure that only experienced mTurk workers from the USA who take their assignments seriously were allowed to participate. *Second*, the pre-screening survey instructions clearly indicated that the respondents should have at least two years of full-time work experience. *Third*, as an additional validity check, the questionnaire asked the participants how much full-time work experience they had.

Fourth, because there were four identical questions in the pre-screening and full-study versions of the instrument, answers to these questions were cross-checked. In several cases when minor discrepancies were observed, the respondents were contacted directly

and asked to complete the instruments again. *Fifth*, the mTurk rules posit that if the requester (i.e. the researcher) is unsatisfied with the quality of the submitted questionnaire, he/she has the right to reject the work without payment. In addition to a monetary loss, this dramatically affects a participant's ranking score and may prevent him/her from enrolling in future projects. Thus, a vast majority of mTurk participants take the completion of survey instruments very seriously. As a result, previous studies show that mTurk participants respond to experimental stimuli in a manner consistent with prior research (Berinsky *et al.*, 2012), and mTurk samples produce results consistent with previous findings (Goodman *et al.*, 2012; Kees *et al.*, 2017). In recent years, mTurk has been frequently used in business research (Feldman and Halali, 2017; Gubler *et al.*, 2017; Parmar *et al.*, 2017), and it was believed that mTurk participants may provide valid data in the context of the present study.

4. Results

4.1 Overview

The results of the pre-screening phase revealed an abundance of knowledge sabotage in the contemporary workplace. Table III shows the percentage of employees who engaged in at least one incident of knowledge sabotage. Most of them were "repeat offenders" because they did so multiple times. It was found that employees engaged in the passive form of knowledge sabotage more often than in its active form.

Respondents who engaged in at least one incident of knowledge sabotage were 37 years old, on average. Fifty-two percent of them were women. They had 13 years of full-time and five years of part-time work experience, ranging from two to over 20 years. In terms of education, 16 per cent had high school or less, 27 per cent had an Associate degree (2-year degree) or some college, 41 per cent a bachelor's degree, 12 per cent a master's degree, and four a doctoral degree.

The respondents provided 177 unique critical incidents. The four exemplars below pertain to each of the four sabotage types:

> P11. I had a supervisor who took advantage of me and my coworkers. He had lied to us regarding the raises and bonuses. He generally mistreated us. He said he needed accurate sales data to give to a regional manager that he was trying to impress so I purposely provided [him] with incorrect information. I acted against my supervisor solely. It embarrassed him. (Provoked-Active)
>
> P83. Someone in my office sent out an email asking a complicated question about a client to some people I am friends with. Although it wasn't to me, I found out about the email and gave her the wrong info. This person had always been very condescending to me and was always an a*s. [This] made her look incompetent. (Unprovoked-Active)
>
> P63. I was working in the Medical Records department and the girl I was training would become my superior. The girl was looking for insurance claim reports on the hard drive and she said she couldn't find it. She asked me about it, but I told her I didn't know where it was, but I did know where it was. I did it because she wasn't nice to me. She liked to give me orders instead of asking me to do

Table III Percentage of employees who ever engaged in knowledge sabotage – phase one (pre-screening)

	Dimension	
	Active (provides wrong knowledge)(%)	*Passive (conceals knowledge)(%)*
Dimension		
Provoked (formal knowledge request)	14.0	26.6
Unprovoked (no formal knowledge request)	14.6	35.7

something. I didn't think it was fair, so I decided I didn't need to offer her any information or help her [. . .] [As a result,] she wasn't able to do her job effectively. (Provoked-Passive)

P94. A colleague in a higher position was needing vital information from my office to complete a yearly report. I was aware that she needed this information, but because of personal issues that her and I have had in the past, and her constant looking down on me as if I was beneath her, I did not provide her with the information. I figured if she didn't ask me directly, there was no reason I needed to provide it. I personally did not care for her. It did delay her completing the report. (Unprovoked-Passive)

Table IV shows the distribution of the types of knowledge sabotage (full-study data). Again, most people did so more than once, and the passive form was more dominant than the active form.

All incidents were analyzed along the following dimensions:

- the target (the entity against which the saboteur acted);
- motivation (what motivated the saboteur to engage in knowledge sabotage);
- impact (the consequences of the saboteur's action); and
- regret (whether the saboteur later regretted her/his action).

A preliminary codebook was developed based on the previous counterproductive workplace behavior literature (Robinson and Bennett, 1995), which is a common technique in qualitative data analysis (Miles and Huberman, 1994). Initially, draft categories of the codes were developed. As data analysis progressed, these codes were continuously refined, merged, and adjusted, and new codes were introduced if needed. The final data analysis was done by two independent coders who had extensive graduate-level training in qualitative research, and an excellent level of inter-rater agreement was achieved (the Krippendorff's (1980) agreement coefficient was over 0.8). In cases of disagreement, the coders discussed the data in person until agreement was reached. Tables V-VIII summarize the findings.

4.2 Target

A vast majority of the saboteurs acted against a particular individual – mostly a colleague; occasionally, a manager; and rarely, a subordinate. Only a small fraction of the saboteurs targeted their organization, and only a few targeted both their organization and an individual simultaneously. The saboteurs engaged in the active form were slightly more likely to target their organization than those in the passive form.

4.3 Motivation

Two distinct motivational factors emerged – external (the external environment, such as other employees, the organization, and the third party) and internal (the saboteurs themselves).

4.3.1 External factors. On average, over two-thirds of the sabotage episodes were motivated by external factors. In terms of *other employees*, several categories emerged. The first pertained to the employees' negative, disruptive, and hostile behavior when they

Table IV Distribution of knowledge sabotage types - phase two (full-study)

	Dimension	
	Active (provides wrong knowledge)(%)	*Passive (conceals knowledge)(%)*
Dimension		
Provoked (formal knowledge request)	16.3	27.1
Unprovoked (no formal knowledge request)	6.8	49.7

Table V Saboteurs' behavior – the provoked-active type

Target	*Motivation*	*Impact*	*Regret*

Colleague (57%)
Manager (23%)
Organization (13%)
Subordinate (7%)
	External factors (65%)
	- Other employees (48%)
	  - Negative behavior (23%)
	  - Negative reciprocation (13%)
	  - Poor performance (13%)
	- Organization (13%)
	  - Negative reciprocation (10%)
	  - Other (3%)
	- Third party (3%)
	Internal factors (35%)
	- Personal gain (19%)
	- Laziness (6%)
	- Lack of time (6%)
	- Other (4%)
		On the person
		Impact: 74%; No impact: 26%
		Impact Type:
		- Official reprimand (19%)
		- Public humiliation (19%)
		- Termination (11%)
		- Time loss (7%)
		- Other (18%)
		On the organization
		Impact: 42%; No Impact: 58%
		Impact type:
		- Time loss (25%)
		- Other (17%)
		On the third party
		- Positive and negative
		On myself
		- Positive and negative
			Yes: 38%
			No: 52%
			Not Sure: 10%

Table VI Saboteurs' behavior – the unprovoked-active type

Target	*Motivation*	*Impact*	*Regret*

Colleague (54%)
Manager (23%)
Organization (15%)
Subordinate (8%)
	External factors (73%)
	- Other employees (73%)
	  - Negative behavior (33%)
	  - Negative reciprocation (27%)
	  - Poor performance (13%)
	Internal factors (27%)
	- Personal gain (27%)
		On the person
		Impact: 80%; No impact: 20%
		Impact type:
		- Official reprimand (24%)
		- Public humiliation (16%)
		- Time loss (16%)
		- Other (24%)
		On the organization
		Impact: 45%; No Impact: 55%
		Impact type:
		- Time loss (20%)
		- Other (25%)
		On the third party
		- None
		On myself
		- Positive and negative
			Yes: 42%
			No: 58%
			Not Sure: 0%

treated their co-workers or subordinates unfairly. It was a major, very consistent reason across all four sabotage types. The blistering quotes below need no further elaboration:

> P1. I work with this horrible person [. . .] I used to try and be nice and put up with her but she is so aggressive and manipulative and actually just a bully.

> P9. I really hated my coworker. The coworker undermined me at every chance he got.

> P10. We had a new manager at work whom EVERYONE detested. He was dour, rude, and worst of all, somehow managed to be a know-it-all even though he was woefully inexperienced.

> P40. [I did it because] I did not respect my supervisor.

> P41. Adam gets on my nerves. He is arrogant and believes he is a know it all.

Table VII Saboteurs' behavior – the provoked-passive type

Target	*Motivation*	*Impact*	*Regret*

Colleague (65%)
Manager (21%)
Organization (10%)
Subordinate (4%)
	External factors (73%)
	- Other employees (64%)
	  - Negative behavior (40%)
	  - Poor performance (20%)
	  - Negative reciprocation (4%)
	- Organization (7%)
	  - Organizational benefit (5%)
	  - Negative reciprocation (2%)
	- Third party (2%)
	Internal factors (27%)
	- Laziness (9%)
	- Envy (4%)
	- Lack of time (4%)
	- Knowledge hoarding (4%)
	- Personal gain (4%)
	- Other (2%)
		On the person
		Impact: 80%; No impact: 20%
		Impact type:
		- Termination (27%)
		- Time loss (22%)
		- Official reprimand (16%)
		- Other (15%)
		On the organization
		Impact: 43%; No impact: 57%
		Impact type:
		- Time loss (22%)
		- Delayed/failed project (7%)
		- Other (14%)
		On the third party
		- Negative
		On myself
		- Positive and negative
			Yes: 29%
			No: 65%
			Not Sure: 6%

Table VIII Saboteurs' behavior – the unprovoked-passive type

Target	*Motivation*	*Impact*	*Regret*

Colleague (60%)
Manager (34%)
Organization (3%)
Subordinate (3%)
	External factors (81%)
	- Other employees (75%)
	  - Negative behavior (28%)
	  - Lack of assistance proactivity (16%)
	  - Poor performance (16%)
	  - Assistance rejection (10%)
	  - Negative reciprocation (5%)
	- Organization (5%)
	  - Organizational benefit (3%)
	  - Other (2%)
	- Third party (1%)
	Internal factors (19%)
	- Lack of time (7%)
	- Reward absence (5%)
	- Laziness (4%)
	- Other (3%)
		On the person
		Impact: 74%; No impact: 26%
		Impact Type:
		- Time loss (27%)
		- Official reprimand (17%)
		- Termination (9%)
		- Other (21%)
		On the organization
		Impact: 57%; No Impact: 43%
		Impact type:
		- Time loss (27%)
		- Delayed/failed project (12%)
		- Other (18%)
		On the third party
		- Negative
		On myself
		- Positive and negative
			Yes: 18%
			No: 74%
			Not Sure: 8%

> P75. A coworker that I loathed and who had undermined and humiliated me in a large group meeting was working on a project [. . .].

Thus, in a situation when the managers or co-workers mentioned above were in need of knowledge from their alleged victims, a logical conclusion would be very simple: Good luck with that!

The second employee-related category pertained to negative reciprocation (especially, in the active form). Negative reciprocation refers to the saboteur's retaliatory actions because the target had previously done exactly the same to the saboteur – for example:

> P3. I had the information but decided not to give it to him [. . .] since he never helped me when I asked in the past.

P51. My direct report manager had done the same for me one time for an important presentation. He apologized but it was insincere and I knew he did it on purpose. I just returned the favor [. . .]

P62. Because she never wanted to help others so I thought she deserved some of the same treatment.

The third category was related to the poor and sub-standard job performance of the target (particularly, in the passive form) – i.e. when the saboteur believed that another employee did not put enough effort into the task, tried to take advantage of others or was incompetent at her/his job. For instance:

P96. He has deliberately tried to not do any work or [put] effort in [the] project.

P22. She already had a copy of it but was too lazy to look for her own quite frankly. People know i'm quite organized and i feel they take advantage of that. At least this person does.

P43. I'm suppose[d] to work alongside an inhouse employee on an account. Well, she knows nothing about the account. I do all the work and have for years.

The fourth category related to the lack of proactivity towards assistance of the person-in-need (in the unprovoked-passive type only). This happened when someone simply failed to approach a knowledge holder for help, but, without a request, the knowledge holder did not wish to voluntarily part with her/his important knowledge. In such situations, the saboteur retaliated against someone's inability to request help when needed. For example:

P87. I knew exactly what they needed to know, but they never took the time to approach me and ask me for help [. . .] I was not about ready to step in and freely offer up my help.

P95. If she didn't feel like asking me about the problem and possible solution then I wasn't going to freely give it.

P35. If they asked for help, I would happily do so; but otherwise, they have to take responsibility for the problem.

P85. I deliberately failed to provide her with information that would have helped [. . .] I retaliated against her inability to ask directly for help.

The last, fifth category pertained to previous assistance rejection (in the unprovoked-passive type only) because the target assumed he/she already had a great degree of expertise, needed no additional assistance, and previously rejected help from others. As a result, nobody wanted to deal with such an individual even after realizing he/she was in dire need:

P45. This happened when a know it all junior person thought that they were god. They didn't need any help from anyone and thought that they were better than you.

P30. [. . .] because I had tried to help her in the past, [but] she always thought she knew everything and did not need my assistance.

P68. She was told countless times "we do things differently here [. . .], please ask if you're having trouble." [T]o which she responded immediately that she felt it was "mansplaining" and the person was being sexist by assuming she didn't know [. . .]

With respect to the motivational factors pertaining to the saboteur's *organization*, negative reciprocation when the saboteur retaliated towards the entire organization occasionally appeared:

P54. I hated the organization I was working for.

P71. I felt that the organization had not treated me as well as I felt it should have.

Surprisingly, in several cases, the saboteurs believed they acted in the best interest of their organization as a whole. In such situations, they did not trust in the target's ability to efficiently or honestly use the provided knowledge or had to manipulate organizational processes to achieve a (positive) desirable outcome. For example:

> P7. I acted against the individual. I had little confidence in the requester to use the information wisely and in an appropriate manner. In particular, I was concerned about recruitment of presenters and attendees, and content being judged out of context.

> P14. I didn't supply the info because I distrusted what it would be used for [. . .] I didn't trust her with potentially damaging info about a parent.

> P53. I did not trust them to place an accurate order so I padded the numbers so they would order too much rather than not enough [. . .] So I would not have to go get more supplies if we ran out.

The saboteurs were also driven by the interest of the third party, but such incidents were very rare.

4.3.2 Internal factors. Personal gain emerged as a leading internal motivational factor in cases of active knowledge sabotage. It included receiving promotions, career advancement, financial gain, easier workload and avoiding punishment for under-performance. For example:

> P27. [. . .] I would not give them my phone number for the rolodex file. It was in my HR file but I did not want to be bothered when off work so when I would see that someone put it in there, I took it out.

> P91. Another sales representative's customer called and asked for information about a product. They asked to speak with their representative and I never gave the representative the message that they called. The customer then called back the next day and I got the sale. [I did this] because I wanted the commission.

Other internal factors included laziness, lack of time, absence of reward, envy and desire to accumulate knowledge, but they were mentioned very rarely.

4.4 Impact

Impact of the saboteur's action was measured with respect to four distinct categories: impact on the person, on the organization, on the third party and on the saboteur her/himself.

Across all four sabotage types, in a majority of incidents, the saboteur's actions consistently had *an impact on the person* who was selected as a target. Official reprimand, when the target received a verbal or written reproof or rebuke from the manager, emerged as a very frequent consequence, particularly in the active form. For example:

> P8. [I]t reflected poorly on his quarterly evaluation.

> P18. [M]y boss got a dressing down for not having completed applications.

> P72. He got called in to the office and was reprimanded severely.

Public humiliation was another type of impact in the active form when the target, after using the wrong knowledge received from the saboteur, looked embarrassed, incompetent or ashamed in front of the other employees. For instance:

> P14. [. . .] it ended up making her look a bit foolish.

> P43. It made her look like she wasn't doing her job.

P59. [. . .] he looked silly for about 15 minutes.

P96. She looked foolish at our meeting.

Time loss was a frequent outcome of the target's application of wrong knowledge or the inability to perform the task efficiently because of missing knowledge. In such situations, time was needlessly wasted even though it was not the primary objective of the saboteur. For example:

P3. It took him a couple of hours of work to gather the info for himself.

P77. So he had to waste twenty minutes of his shift.

Termination, when the target was fired or resigned, also emerged as an outcome of the saboteur's action:

P6. She ended up getting fired the next week.

P28. The engineer looked like a fool and he left the company shortly after.

P98. He eventually was asked to either leave the organization or go on an Improvement plan. He chose to leave the company.

In addition, several other factors were mentioned, such as making the target very upset, putting her/him under pressure, and making her/him lose trust in her/his colleagues. None of them, however, was mentioned frequently enough to warrant a distinct category.

Generally, about a half of all incidents had *an impact on the saboteur's organization*, even though this was rarely the saboteur's intention. Time loss was the dominating factor because, every time an employee had to re-do the task or performed the task in an inefficient way, her/his time was wasted, but this happened at the expense of the entire organization. Consider, for example, the following incidents:

P64. The most vivid memory I have of this is regarding a fellow employee. He had been quite a bit of a rude bully in multiple previous encounters. He was delivering a load of industrial pipe to a location. I conveniently skipped mentioning they had no forklift there, and the employee didn't bother putting the mobile forklift on the truck. He ended up having to use the wood beams and manually unload the truck.

P13. [. . .] I gave the wrong information to a guy who was annoying the crap out of me. . . he was a smart mouth and always wanted to be boss [. . .] [and he] lost some time driving around looking for the right address.

P89. My boss was going to meet with ou[r] tax attorneys about an audit. I knew he would need a breakdown of all the taxes we had paid the prior year. I always tried to have things ready for him in advance, to anticipate what he might need. He always complained that I "jumped the gun" [. . .] So I decided this time I wouldn't give it without being asked and I wouldn't remind him he needed it [. . .] He went into the meeting without it and had to have a follow up meeting to go over it once he had the information.

In all of these incidents, the saboteurs targeted another individual solely because of her/his negative workplace behavior or being unreceptive to prior assistance. As a result of the retaliatory actions, the targets had to work harder and longer by manually unloading the truck, driving extra time looking for the correct address or arranging an additional meeting, which consumed their paid worktime and made the organization less efficient.

In a similar vein, a failed or delayed project was another unanticipated by-product of the saboteur's action – for example:

P23. A fellow manager that I didn't get along with asked me for assistance on a project a few years ago. I knew he needed the help and deserved my assistance. I also knew he had been a pain in the b*tt to me for several years. I declined to help, I claimed I was too busy although I did it in such a way that it was quite clear it was for personal reasons [. . .] the guy had been a jerk to me for years [. . .] The project ultimately failed.

P66. Woman I work with, she's a lazy slob, volunteers for huge projects and then tries to get other people to help her look good because she doesn't know [how] to do the work she volunteered for. I could have helped her complete a project in 10 minutes, that would take her a week, but I didn't, because I literally hate this woman [and] she dropped the ball on the project.

P92. A new worker had needed some assistance on a task that he was not familiar with, we were all on a time line. I chose to prioritize my time differently because I felt he was difficult to work with and left him out. It caused a big problem [. . .] They didn't complete the task properly on time.

P52. A co-worker was missing a piece of code for our web design project. I could have easily provided him with the code, but I did not. I wanted to let him figure it out on his own [because] the co-worker has been mean to me in the past. [In the result,] one of our web design projects was delayed for a while.

Again, the saboteurs acted against a single individual, but this had extremely negative consequences for the entire organization when the project was terminated or delayed.

The "other" category of organizational impacts included lost opportunities and clients, waste of money, extra hiring expenses, products being out-of-stock, understaffing and lower quality of products or services. For instance:

P36. A co-worker was working on a marketing proposal for a school district that was looking for architectural services for various district projects [. . .] This co-worker and I didn't get along because she was a rude, obnoxious know-it-all. Our proposal templates are in a program that she wasn't familiar with so she was having great difficultly trying to get the proposal done before the deadline. Instead of asking me for help she went around to others and ask[ed for] their assistance. All of them told her to seek my help, which she wouldn't, because she didn't want me to know she couldn't figure it out on her own. So because she didn't ask me, I didn't offer my help, in fact, I avoided helping her at all. Needless to say, her proposal was terrible and not organized at all. The impact to the organization was that we didn't get the project.

P74. I was to show another employee how to make various flavors of our product. I made her copies of all the recipe sheets, but they didn't include changes I had made to tweak the flavors better over the years. I withheld those on purpose. I had made those tweaks over many years and felt like that information was mine and not the company's. The product made by this person was not the same or as good.

At the same time, when the saboteur acted in the best interest of her/his organization, there was a positive outcome of her/his actions. For example, in the following incident, the final outcome was the improvement of quality standards for the entire organization:

P33. I was a manager in the quality control department. Another manager, from the Operations department, asked for a metric report to support his agenda in cross training some of our current staff to new skills. I refused to provide this data. Although it would help him make his case, it was counter-productive to my department's needs for quality control. It delayed the cross training program he was trying to initiate which, in turn, led to higher company-wide quality standards to be achieved.

On rare occasions, the saboteur's actions had an unanticipated (mostly negative) impact on the third party – usually on clients or customers. For example:

P5. In an office setting where I was working with a peer who was simply rude and was sure she knew it all. She forgot to file some information for a client, but since she was never open to

> anything I had to say I deliberately kept my mouth shut. It meant that the filings were late[,] the client was unhappy and we had to pay a penalty.

> P19. A coworker from the same department as me was hosting one of our foreign clients for dinner one evening. It was my turn to host the dinner but she somehow convinced management to let her do it. She asked me for advice as to where to bring them and I gave her the name of a restaurant in a terrible part of town that had been long closed. We live in a large city and she wasn't native to there so she was unfamiliar with any of it. The client was frustrated and angry.

In several incidents, the subjects reported positive and negative impacts of their actions on themselves. Whereas the positive outcomes were planned and desirable, the negative outcomes were not. For example, in the incident below, the saboteur deliberately offered her/his advice to reduce her/his workload while disregarding the resulting higher costs for the entire organization:

> P56. Towards the end of the work year, we needed to decide where to fulfill our purchase orders. Not requested from me, I chose to give my own advice on which equipment to purchase which resulted in an easier workload but cost the organization more.

In another incident, the saboteur had to suffer the consequences of her/his action in the form of a pay reduction, in addition to the negative impact on other employees who lost their jobs:

> P65. I purposely did not share the information I knew this coworker was looking for to complete a report she had due. She never asked me for it but I did know she was looking for it. I did not like this person personally and I thought this was a good way to sabotage her good reputation. This person was a show off and I was jealous of her place in the company. The company ended up losing a big account and it caused a pay reduction to those who were not fired. In the end I lost wages and regretted having done this. KARMA got me back soon after I did this. The company had major losses due to this.

In other similar incidents where the saboteurs lost their jobs, were reprimanded, or lost bonus pay, none of them anticipated such dramatic negative outcomes of their presumably trivial counterproductive knowledge behavior.

4.5 Regret

Overall, only 26 per cent of the saboteurs regretted their behavior. More expressed regret about an active than a passive form of sabotage. All of the saboteurs who personally faced the negative consequences of their action regretted their behavior. In contrast, almost all who enjoyed a positive personal outcome did not regret their action. No other patterns between regret and other dimensions – such as the target, motivation, and impact – emerged.

5. Discussion

The purpose of this study is to conceptualize the phenomenon of knowledge sabotage, to develop its typology, and to empirically demonstrate the existence of this counterproductive knowledge behavior in the contemporary organization. For this, 100 respondents with at least two years of full-time work experience reported 177 critical incidents which were subjected to qualitative data analysis. The findings identified several theoretical and practical implications that warrant further elaboration.

5.1 Implications for theory

First, the pre-screening survey indicated that 42 per cent of employees had engaged in knowledge sabotage – an astonishingly high number. Moreover, most of them did so more

than once, which confirms the existence of knowledge sabotage in the contemporary organization as an extreme form of counterproductive workplace behavior. The extant literature presents a variety of counterproductive knowledge behaviors – disengagement from knowledge sharing (Ford *et al.*, 2015), knowledge sharing ignorance (Israilidis *et al.*, 2015), partial knowledge sharing (Ford and Staples, 2010), knowledge hoarding (Evans *et al.*, 2015), counter-knowledge sharing (Cegarra-Navarro *et al.*, 2015; Martelo-Landroguez *et al.*, 2019), and knowledge hiding (Connelly *et al.*, 2012) – and the present study extends the list above by empirically confirming the existence of knowledge sabotage.

Second, the results validate the proposed typology of knowledge sabotage where incidents are positioned within a two-by-two matrix along the following dimensions:

- provoked (reactive – when the target directly approached the saboteur) vs. unprovoked (proactive – when the target did not approach the saboteur); and
- active (action – when the saboteur provides incorrect critical knowledge) vs. passive (inaction – when the saboteur conceals critical knowledge).

Consistent with prior reports on counterproductive workplace behavior (Maylett, 2017), more employees were found to be engaged in the passive than in the active form of knowledge sabotage. This finding is not surprising because most people are "cognitive misers" who tend to save mental resources (Fiske and Taylor, 1984; West, 2008) and avoid unnecessary tasks: whereas the active form of knowledge sabotage requires extra action to fabricate (mental effort) and provide (physical effort) wrong knowledge, the passive form requires less effort and is, therefore, easier to perform.

In addition, deterrence theory suggests that people make rational decisions by considering the relative costs and benefits associated with an illicit action (Geerken and Gove, 1975; Pratt *et al.*, 2006). Particularly, individuals estimate the degree of certainty, severity and swiftness of a punishment, which together serve as action deterrents. The punishment may be formal (e.g. a reprimand, a termination) or informal (e.g. an unpleasant conversation with the target). In cases of active knowledge sabotage, the target may eventually track the wrong knowledge back to its source to demonstrate the damaging behavior of the saboteur, but proving one's inaction and its consequences is more difficult. The punishment for a deliberately wrong action is also generally more severe than that for an inaction, and it takes a long time for the target to realize the maliciousness of one's inaction. Thus, the certainty, severity and swiftness of punishment may serve as a deterrent to active knowledge sabotage.

Third, the present study revealed that knowledge sabotage rarely takes the form of retaliatory behavior against one's organization. It was found that knowledge saboteurs seldom target their organizations; this happened in only around ten per cent of all incidents, and the saboteurs were extremely rarely motivated by organizational issues. Instead, knowledge saboteurs mostly acted against their fellow co-workers; sometimes, against their managers; and, in rare cases, against their subordinates. Approximately one-half of all incidents were caused by interpersonal issues, mostly resulting from the target's previous hostile behavior, failure to provide assistance, and poor performance (from the saboteur's perspective). As such, knowledge sabotage is often expressed in the form of revenge against a particular individual – a phenomenon referred to at as reciprocal deviance, which is founded on motives of revenge (Kemper, 1966). The quotes presented in the Results section convey a great degree of the saboteurs' frustration with their colleagues, and the saboteurs used this disappointment to justify their illicit actions.

The broaden-and-build theory posits that positive and negative emotions have different cognitive and behavioral effects (Fredrickson, 2001). Positive workplace emotions, which may result from desirable co-workers' behavior, broaden employees' thought-action repertoires, increase their cognitive resources and improve positive reciprocation tendencies. In sharp

contrast, negative workplace emotions – which may be triggered by harmful colleagues' actions – narrow people's thought-action repertoires, facilitate offensive action and force negative reciprocation. Prior research also suggests that feelings of revenge are ruminative and originate from the discrepancies between the present state (e.g. being frequently humiliated by a colleague) and central goals that are difficult to attain (e.g. desire to work in a collegial environment) (Orth and Montada, 2006). Thus, knowledge sabotage incidents are not random or automatic actions; instead, they are well-thought-out, deliberate, and possibly planned attempts to undermine the workplace enemy. This confirms the recent findings by Serenko and Bontis (2016) who empirically demonstrated that employees may intentionally reciprocate both positive and negative knowledge behaviors of their colleagues.

Fourth, a small yet noticeable proportion of knowledge saboteurs are driven by personal, ego-driven motives, such as career advancement, comfortable workload, financial reward and punishment avoidance. These incidents resemble those of traditional workplace sabotage when employees engage in counterproductive behavior solely for the sake of some personal benefits. By doing so, they disregard the overall organizational objectives and focus on themselves only (Robinson and Bennett, 1995).

Fifth, a majority of all incidents had a negative impact on other employees who were reprimanded, humiliated, and even terminated. Some knowledge saboteurs managed to achieve personal gains, which were the intended consequences of their behavior. Nevertheless, even though only a small fraction of knowledge saboteurs purposely acted against their organizations, approximately one-half of all incidents produced negative organizational impacts, referred to as unintended harm. The key types of negative impacts included time loss and failed or delayed projects, followed by lost clients, waste of money, increased hiring costs, products being out-of-stock, understaffing, and poor quality of products or services. This points to two issues: the actual cost of knowledge sabotage and the attribution of intention to damage the organization.

With respect to the cost of knowledge sabotage, time losses (when the target has to perform inefficient tasks, re-do some work, look for information elsewhere and distract others asking for advice) are directly linked to organizational expenses and productivity. Delayed or even failed projects result in a waste of financial resources. Being out-of-stock, being under-staffed, and having poor product or service quality are directly linked to lower customer satisfaction, which, in turn, increases customer attrition and decreases profit. The cost of hiring a replacement for a worker who was terminated or who left as a result of knowledge sabotage typically ranges from US$5,000 to US$17,000 (Blatter *et al.*, 2012). At the same time, it is unlikely that the saboteurs who engaged in a relatively inconsequential behavior (from the perspective of their entire organization) to retaliate against a bad employee realized the actual magnitude and cost of their action.

As discussed above, a vast majority of the saboteurs had no intention of harming their organization. However, observers attribute the intentionality depending on the valence of the consequences of an action: they tend to believe that people act deliberately in cases of negative impacts or undesirable side effects regardless of their actual intentions to cause harm (Knobe, 2003; Bauman, 2011). This means that the management and co-workers who realize the negative organizational impact of the saboteur's behavior are likely to assume that it was the actual saboteur's intention to harm not only a particular individual but also the entire organization. This, in turn, may result in a severe disciplinary action against the culprit.

Sixth, overall, only a minority of the saboteurs regretted their decision. Regret is a negative, cognitive emotion that individuals experience upon realizing that they should have acted differently (Zeelenberg, 1999). It was found that more saboteurs regretted active than passive knowledge sabotage behavior. This finding is consistent with the literature because outcome achieved through action generally leads to more regret than that resulting from

inaction (Gilovich and Medvec, 1995). Most likely, the saboteurs perceived a passive form of sabotage as less damaging. They also engaged in passive sabotage more frequently and, therefore, were more familiar with it and were less likely to elaborate on their inaction afterwards. In other words, knowledge saboteurs consider the passive form of knowledge sabotage more common and less extreme.

Seventh, the findings indicate that, in a few exceptional cases, the saboteurs acted in the interest of their organization. As such, they had to sabotage their superior or colleague for the benefit of their entire organization. Bouty (2000) observed similar behavior when individuals engaged in counterproductive knowledge behavior to protect the interests of their overall organization. This shows that, whereas a vast majority of knowledge sabotage incidents are driven by malicious intentions, there may be exceptions to this rule.

Eighth, the knowledge management literature suggests that productive and counterproductive knowledge behaviors are not opposites of each other. For example, knowledge sharing and knowledge hiding are distinct constructs which are motivated by different factors (Connelly *et al.*, 2012). Consistent with this line of reasoning, the present study argues that knowledge sabotage is not an opposite side of well-known productive knowledge behaviors, particularly knowledge sharing. Common individual-level knowledge sharing barriers include job insecurity, unawareness of knowledge-sharing benefits, desire for power, low tolerance for mistakes, insufficient personal interaction, lower trust, inefficient communication and differences in age, gender, education and social status (Riege, 2005; Serenko, Bontis and Hardie, 2007). None of these knowledge sharing barriers were observed as the factors motivating knowledge sabotage, which empirically confirms the unique nature of this concept.

Last, the present study confirmed that the Critical Incident Technique is a robust and rigorous inquiry method which may be fruitfully applied to study counterproductive workplace behavior. The Critical Incident Technique was used to identify and analyze a number of knowledge sabotage incidents, and it allowed documenting highly memorable, first-hand employee experience that took place in the workplace to generate both theoretical insights and practical recommendations. Thus, future researchers focusing on counterproductive workplace behavior are advised to consider the use of this technique as a lens of analysis.

5.2 Implications for practice

Managers should be aware of the phenomenon of knowledge sabotage and realize that, at some point, almost a half of their employees will engage in it. Given the covert nature of the passive type of knowledge sabotage, many incidents may go unnoticed and management may never realize the harm that was inflicted upon the other employees and the entire organization. To address and prevent this burdensome problem, organizations are recommended to develop a strategy with the goal to prevent inter-employee knowledge sabotage. This strategy should focus on the following broad areas: conducting employee surveys, offering employee education, providing victim assistance, creating a friendly and collaborative environment, and developing relevant policies.

First, including knowledge sabotage-related questions in annual employee surveys is recommended. Select organizations already cover general instances of workplace sabotage in such surveys (Maylett, 2017), and the addition of knowledge sabotage-specific questions may shed light on the dark side of organizational life and help management develop proactive solutions. Given that knowledge sabotage is considered an extremely negative behavior, some employees may not want to admit it even in anonymous surveys due to social desirability bias. To address this issue, employee surveys should also inquire about situations when the respondents not only committed the acts of knowledge sabotage but also were its victims.

Second, due to the covert nature of passive knowledge sabotage incidents, some employees may fail to recognize the wrongdoing of their colleagues, subordinates, or managers or assume that such behavior is normal within the boundaries of their organization. Thus, it is very important to teach employees how to recognize incidents of knowledge sabotage and inform them about the actions that need to be taken. For example, they may report the counterproductive colleague's behavior to their managers who, in turn, may take a corrective action. In this case, the victim is less likely to engage in negative reciprocation by committing an act of knowledge sabotage as a form of retaliation. Another way to tackle the problem is by educating employees by explaining the individual and organizational consequences of knowledge sabotage. In such instances, employees may regret their previous incidents of knowledge sabotage, and this may reduce their probability of engaging in new ones. It is also important to teach employees to approach their colleagues for assistance because, when they fail to do so, others are more likely to engage in knowledge sabotage and ignore one's need for knowledge.

Third, organizations should develop victim assistance programs to help the targets of knowledge sabotage. Severe episodes of knowledge sabotage may lead to voluntary or involuntary job termination because victims become so disappointed with their workplace that they choose to leave it, or they fail to prove the benevolence of their intentions when they applied wrong knowledge which damaged their organization. Such victim assistance programs may include a formal, unbiased review process and assign a neutral ombudsperson who may help the management team look at the situation from various perspectives. This, in turn, may reduce the turnover rate which would result in better knowledge retention and higher organizational performance.

Fourth, managers should realize that the best way to reduce knowledge sabotage is to improve inter-personal relationships among their employees and to foster a friendly and collaborative environment. They need to identify conflict-prone individuals and under-performers and formally deal with them instead of letting their subordinates take measures into their own hands by using knowledge sabotage as a means to penalize someone. They should also listen to the needs of their employees because, at least in some cases, management can re-engineer organizational processes to ease the workload and eliminate unnecessary tasks to make sure employees will not try to sabotage their organization.

Last, to ensure the long-term success of the initiatives above, organizations are recommended to follow a comprehensive policy-based approach instead of dealing with knowledge sabotage issues on a one-on-one basis as they arise. Most organizations have already successfully implemented various policies aimed at improving inter-employee interactions, and the development of anti-knowledge sabotage policies may send a strong message to all employees and prevent the costly incidents documented in the present study. In addition, knowledge sabotage policies should be included in knowledge management maturity models which are used to formally assess the quality of organizational knowledge management activities (Hsieh, Lin and Lin, 2009; Serenko, Bontis and Hull, 2016).

5.3 Limitations

Despite its novelty and contribution, this study had several limitations. First, only individuals residing in the USA were allowed to participate in this study. It is possible that national culture (Hofstede, 1980) shapes the way employees engage in counterproductive workplace behavior, and, therefore, the findings may not be generalizable. Of particular importance is the individualism vs collectivism dimension because it may change both the antecedents and consequences of knowledge sabotage behavior. Therefore, it is recommended that future researchers conduct similar studies in other countries, especially in those with collectivistic cultures. Second, this investigation approached the issue from the perspective of knowledge saboteurs. However, their targets may have different perceptions

of the same situation and may offer new insights. Thus, it is recommended that future scholars focus their empirical work on the targets of knowledge sabotage. Third, this study identified a number of general individual- and organizational-level impacts of knowledge sabotage, but it would be interesting to calculate their exact costs. Fourth, it is likely that knowledge sabotage may dominate particular types of organizations, specifically in the public sector, and its consequences may be more far-reaching for knowledge-intensive organizations where knowledge represents the most important organizational asset. It is, therefore, recommended that future researchers explore the avenues above.

6. Conclusion

The extant literature generally depicts a workplace saboteur as a disgruntled employee who is trying to get revenge on her/his organization by engaging in various malicious acts – all done with the purpose of penalizing the organization, its customers, and its loyal employees. The present study shows that such a description does not universally apply to a knowledge saboteur: this is an individual driven by a feeling of revenge against a hostile, unhelpful, and unproductive co-worker or manager with the key goal being to harm or humiliate the (presumed) culprit. Such saboteurs rarely regret their behavior, which often results in undesirable negative consequences for their organization, including lost efficiency, damaged employee morale, waste of resources and unnecessary financial expenses. Some incidents of sabotage lead to delayed or even terminated projects – which, however, is not the saboteur's objective. Given that over 40 per cent of all employees in the USA engage in knowledge sabotage, it is recommended that managers pay attention to the issue and that researchers continue the line of inquiry introduced in the present study.

References

Abubakar, A.M. and Arasl, H. (2016), "Dear top management, please don't make me a cynic: intention to sabotage", *Journal of Management Development*, Vol. 35 No. 10, pp. 1266-1286.

Ambrose, M.L., Seabright, M.A. and Schminke, M. (2002), "Sabotage in the workplace: the role of organizational injustice", *Organizational Behavior and Human Decision Processes*, Vol. 89 No. 1, pp. 947-965.

Analoui, F. (1995), "Workplace sabotage: its styles, motives and management", *Journal of Management Development*, Vol. 14 No. 7, pp. 48-65.

Andersson, L.M. and Pearson, C.M. (1999), "Tit for tat? The spiraling effect of incivility in the workplace", *Academy of Management Review*, Vol. 24 No. 3, pp. 452-471.

Andreeva, T. and Kianto, A. (2012), "Does knowledge management really matter? Linking knowledge management practices, competitiveness and economic performance", *Journal of Knowledge Management*, Vol. 16 No. 4, pp. 617-636.

Ardichvili, A., Maurer, M., Li, W., Wentling, T. and Stuedemann, R. (2006), "Cultural influences on knowledge sharing through online communities of practice", *Journal of Knowledge Management*, Vol. 10 No. 1, pp. 94-107.

Bartlett, J.E. and Bartlett, M.E. (2011), "Workplace bullying: an integrative literature review", *Advances in Developing Human Resources*, Vol. 13 No. 1, pp. 69-84.

Bauman, D.C. (2011), "Evaluating ethical approaches to crisis leadership: insights from unintentional harm research", *Journal of Business Ethics*, Vol. 98 No. 2, pp. 281-295.

Bennett, R.J., Aquino, K., Reed, A. and Thau, S. (2005), "The normative nature of employee deviance and the impact of moral identity", in Fox, S. and Spector, P.E. (Eds), *Counterproductive Work Behavior: Investigations of Actors and Targets*, American Psychological Association, Washington, DC, pp. 107-125.

Berinsky, A.J., Huber, G.A. and Lenz, G.S. (2012), "Evaluating online labor markets for experimental research: Amazon.com's mechanical Turk", *Political Analysis*, Vol. 20 No. 3, pp. 351-368.

Blatter, M., Muehlemann, S. and Schenker, S. (2012), "The costs of hiring skilled workers", *European Economic Review*, Vol. 56 No. 1, pp. 20-35.

Bock, G.-W., Zmud, R.W., Kim, Y.-G. and Lee, J.-N. (2005), "Behavioral intention formation in knowledge sharing: Examining the rules of extrinsic motivators, social-psychological forces, and organizational climate", *MIS Quarterly*, Vol. 29 No. 1, pp. 87-111.

Boddy, C.R. (2011), "Corporate psychopaths, bullying and unfair supervision in the workplace", *Journal of Business Ethics*, Vol. 100 No. 3, pp. 367-379.

Boddy, C.R. (2014), "Corporate psychopaths, conflict, employee affective well-being and counterproductive work behaviour", *Journal of Business Ethics*, Vol. 121 No. 1, pp. 107-121.

Bogilović, S., Černe, M. and Škerlavaj, M. (2017), "Hiding behind a mask? Cultural intelligence, knowledge hiding, and individual and team creativity", *European Journal of Work and Organizational Psychology*, Vol. 26 No. 5, pp. 710-723.

Bouty, I. (2000), "Interpersonal and interaction influences on informal resource exchanges between R&D researchers across organizational boundaries", *Academy of Management Journal*, Vol. 43 No. 1, pp. 50-65.

Brock, M.E., Martin, L.E. and Buckley, M.R. (2013), "Time theft in organizations: the development of the time banditry questionnaire", *International Journal of Selection and Assessment*, Vol. 21 No. 3, pp. 309-321.

Bruursema, K., Kessler, S.R. and Spector, P.E. (2011), "Bored employees misbehaving: the relationship between boredom and counterproductive work behaviour", *Work & Stress*, Vol. 25 No. 2, pp. 93-107.

Buenechea-Elberdin, M., Sáenz, J. and Kianto, A. (2018), "Knowledge management strategies, intellectual capital, and innovation performance: a comparison between high- and low-tech firms", *Journal of Knowledge Management*, Vol. 22 No. 8, pp. 1757-1781.

Buhrmester, M., Kwang, T. and Gosling, S.D. (2011), "Amazon's mechanical Turk: a new source of inexpensive, yet high-quality, data?", *Perspectives on Psychological Science: a Journal of the Association for Psychological Science*, Vol. 6 No. 1, pp. 3-5.

Bundred, S. (2006), "Solutions to silos: joining up knowledge", *Public Money & Management*, Vol. 26 No. 2, pp. 125-130.

Buss, A.H. (1961), *The Psychology of Aggression*, Wiley, New York, NY.

Butterfield, L.D., Borgen, W.A., Amundson, N.E. and Maglio, A.-S.T. (2005), "Fifty years of the critical incident technique: 1954-2004 and beyond", *Qualitative Research*, Vol. 5 No. 4, pp. 475-497.

Butterworth, H. (2017), *The Story of Magellan and the Discovery of the Philippines*, CreateSpace Independent Publishing Platform, London.

Byrne, A., Barling, J. and Dupré, K.E. (2014), "Leader apologies and employee and leader well-being", *Journal of Business Ethics*, Vol. 121 No. 1, pp. 91-106.

Cegarra-Navarro, J.-G., Cepeda-Carrión, G. and Wensley, A. (2015), "Negative aspects of counter-knowledge on absorptive capacity and human capital", *Journal of Intellectual Capital*, Vol. 16 No. 4, pp. 763-778.

Černe, M., Hernaus, T., Dysvik, A. and Škerlavaj, M. (2017), "The role of multilevel synergistic interplay among team mastery climate, knowledge hiding, and job characteristics in stimulating innovative work behavior", *Human Resource Management Journal*, Vol. 27 No. 2, pp. 281-299.

Černe, M., Nerstad, C.G.L., Dysvik, A. and Škerlavaj, M. (2014), "What goes around comes around: knowledge hiding, perceived motivational climate, and creativity", *Academy of Management Journal*, Vol. 57 No. 1, pp. 172-192.

Cohen, A. (2016), "Are they among us? A conceptual framework of the relationship between the dark triad personality and counterproductive work behaviors (CWBs)", *Human Resource Management Review*, Vol. 26 No. 1, pp. 69-85.

Connelly, C.E. and Zweig, D. (2015), "How perpetrators and targets construe knowledge hiding in organizations", *European Journal of Work and Organizational Psychology*, Vol. 24 No. 3, pp. 479-489.

Connelly, C.E., Zweig, D., Webster, J. and Trougakos, J.P. (2012), "Knowledge hiding in organizations", *Journal of Organizational Behavior*, Vol. 33 No. 1, pp. 64-88.

Coye, R.W., Murphy, P.J. and Spencer, P.E. (2010), "Using historic mutinies to understand defiance in modern organizations", *Journal of Management History*, Vol. 16 No. 2, pp. 270-287.

Crino, M.D. (1994), "Employee sabotage: a random or preventable phenomenon?", *Journal of Managerial Issues*, Vol. 6 No. 3, pp. 311-330.

Crowne, D.P. and Marlowe, D. (1960), "A new scale of social desirability independent of psychopathology", *Journal of Consulting Psychology*, Vol. 24 No. 4, pp. 349-354.

Dalal, R.S. (2005), "A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior", *Journal of Applied Psychology*, Vol. 90 No. 6, pp. 1241-1255.

de Geofroy, Z. and Evans, M.M. (2017), "Are emotionally intelligent employees less likely to hide their knowledge?", *Knowledge and Process Management*, Vol. 24 No. 2, pp. 81-95.

Donate, M.J. and Guadamillas, F. (2015), "An empirical study on the relationships between knowledge management, knowledge-oriented human resource practices and innovation", *Knowledge Management Research & Practice*, Vol. 13 No. 2, pp. 134-148.

Evans, J.M., Hendron, M.G. and Oldroyd, J.B. (2015), "Withholding the ace: the individual- and unit-level performance effects of self-reported and perceived knowledge hoarding", *Organization Science*, Vol. 26 No. 2, pp. 494-510.

Fang, Y.-H. (2017), "Coping with fear and guilt using mobile social networking applications: knowledge hiding, loafing, and sharing", *Telematics and Informatics*, Vol. 34 No. 5, pp. 779-797.

Feldman, Y. and Halali, E. (2017), "Regulating 'good' people in subtle conflicts of interest situations", *Journal of Business Ethics*, Vol. 154 No. 1, pp. 1-19.

Fiske, S.T. and Taylor, S.E. (1984), *Social Cognition*, Longman Higher Education, London.

Flanagan, J.C. (1954), "The critical incident technique", *Psychological Bulletin*, Vol. 5 No. 4, pp. 327-358.

Fong, P.S.W., Men, C., Luo, J. and Jia, R. (2018), "Knowledge hiding and team creativity: the contingent role of task interdependence", *Management Decision*, Vol. 56 No. 2, pp. 329-343.

Ford, D., Myrden, S.E. and Jones, T.D. (2015), "Understanding 'disengagement from knowledge sharing': engagement theory versus adaptive cost theory", *Journal of Knowledge Management*, Vol. 19 No. 3, pp. 476-496.

Ford, D.P. and Staples, S. (2010), "Are full and partial knowledge sharing the same?", *Journal of Knowledge Management*, Vol. 14 No. 3, pp. 394-409.

Fredrickson, B.L. (2001), "The role of positive emotions in positive psychology: the broaden-and-build theory of positive emotions", *American Psychologist*, Vol. 56 No. 3, pp. 218-226.

Gameson, R., Suresh, S. and Chinyio, E. (2008), "Project debriefing: a multi-domain review of practices and procedures", *Proceedings of the 24th Annual Association of Researchers in Construction Management Conference. A. Dainty, Cardiff*, pp. 329-338.

Gaviria-Marin, M., Merigo, J.M. and Popa, S. (2018), "Twenty years of the journal of knowledge management: a bibliometric analysis", *Journal of Knowledge Management*, Vol. 22 No. 8, pp. 1655-1687.

Geerken, M.R. and Gove, W.R. (1975), "Deterrence: some theoretical considerations", *Law & Society Review*, Vol. 9 No. 3, pp. 497-513.

Giacalone, R.A. and Knouse, S.B. (1990), "Justifying wrongful employee behavior: the role of personality in organizational sabotage", *Journal of Business Ethics*, Vol. 9 No. 1, pp. 55-61.

Gilovich, T. and Medvec, V.H. (1995), "The experience of regret: what, when, and why", *Psychological Review*, Vol. 102 No. 2, pp. 379-395.

Goodman, J.K., Cryder, C.E. and Cheema, A. (2012), "Data collection in a flat world: strengths and weaknesses of mechanical Turk samples", in Gürhan-Canli, Z., Otnes, C. and Zhu, R. (Eds), *Advances in Consumer Research*, Association for Consumer Research, Duluth, MN, pp. 112-116.

Greenberg, J. (1990), "Employee theft as a reaction to underpayment inequity: the hidden cost of pay cuts", *Journal of Applied Psychology*, Vol. 75 No. 5, pp. 561-568.

Gubler, J.R., Herrick, S., Price, R.A. and Wood, D.A. (2017), "Violence, aggression, and ethics: the link between exposure to human violence and unethical behavior", *Journal of Business Ethics*, Vol. 147 No. 1, pp. 1-10.

Hari, S., Egbu, C. and Kumar, B. (2005), "A knowledge capture awareness tool: an empirical study on small and medium enterprises in the construction industry", *Engineering, Construction and Architectural Management*, Vol. 12 No. 6, pp. 533-567.

Harris, L.C. (2002), "Sabotaging market-oriented culture change: an exploration of resistance justifications and approaches", *Journal of Marketing Theory and Practice*, Vol. 10 No. 3, pp. 58-74.

Harvey, M., Treadway, D., Heames, J.T. and Duke, A. (2009), "Bullying in the 21st century global organization: an ethical perspective", *Journal of Business Ethics*, Vol. 85 No. 1, pp. 27-40.

Heisig, P., Suraj, O.A., Kianto, A., Kemboi, C., Arrau, G.P. and Easa, N.F. (2016), "Knowledge management and business performance: global experts' views on future research needs", *Journal of Knowledge Management*, Vol. 20 No. 6, pp. 1169-1198.

Henrie, M. and Hedgepeth, O. (2003), "Size is important in knowledge management", *Journal of Knowledge Management Practice*, Vol. 4.

Hernaus, T., Cerne, M., Connelly, C., Vokic, N.P. and Škerlavaj, M. (2019), "Evasive knowledge hiding in academia: when competitive individuals are asked to collaborate", *Journal of Knowledge Management*, Vol. 23 No. 4, pp. 597-618.

Hislop, D. (2003), "Linking human resource management and knowledge management via commitment: a review and research agenda", *Employee Relations*, Vol. 25 No. 2, pp. 182-202.

Hobbs, N. (1948), "The development of a code of ethical standards for psychology", *American Psychologist*, Vol. 3 No. 3, pp. 80-84.

Hofstede, G.H. (1980), *Culture's Consequences: International Differences in Work-Related Values*, Sage Publications, Beverly Hills, CA.

Holten, A.-L., Hancock, G.R., Persson, R., Hansen, Å.M. and Høgh, A. (2016), "Knowledge hoarding: antecedent or consequent of negative acts? The mediating role of trust and justice", *Journal of Knowledge Management*, Vol. 20 No. 2, pp. 215-229.

Hsieh, P.J., Lin, B. and Lin, C. (2009), "The construction and application of knowledge navigator model (KNM^{TM}): an evaluation of knowledge management maturity", *Expert Systems with Applications*, Vol. 36 No. 2, pp. 4087-4100.

Huo, W., Cai, Z., Luo, J., Men, C. and Jia, R. (2016), "Antecedents and intervention mechanisms: a multi-level study of R&D team's knowledge hiding behavior", *Journal of Knowledge Management*, Vol. 20 No. 5, pp. 880-897.

Israilidis, J., Siachou, E., Cooke, L. and Lock, R. (2015), "Individual variables with an impact on knowledge sharing: the critical role of employees' ignorance", *Journal of Knowledge Management*, Vol. 19 No. 6, pp. 1109-1123.

Jha, J.K. and Varkkey, B. (2018), "Are you a cistern or a channel? Exploring factors triggering knowledge-hiding behavior at the workplace: evidence from the Indian R&D professionals", *Journal of Knowledge Management*, Vol. 22 No. 4, pp. 824-849.

Jones, S.E. (2013), *Against Technology: From the Luddites to Neo-Luddism*, Routledge, New York, NY.

Kang, S.-W. (2016), "Knowledge withholding: psychological hindrance to the innovation diffusion within an organisation", *Knowledge Management Research & Practice*, Vol. 14 No. 1, pp. 144-149.

Kao, F.-H., Cheng, B.-S., Kuo, C.-C. and Huang, M.-P. (2014), "Stressors, withdrawal, and sabotage in frontline employees: the moderating effects of caring and service climates", *Journal of Occupational and Organizational Psychology*, Vol. 87 No. 4, pp. 755-780.

Keashly, L. and Harvey, S. (2005), "Emotional abuse in the workplace", in Fox, S. and Spector, P.E. (Eds), *Counterproductive Work Behavior: Investigations of Actors and Targets*, American Psychological Association, Washington, DC, pp. 201-235.

Kees, J., Berry, C., Burton, S. and Sheehan, K. (2017), "An analysis of data quality: professional panels, student subject pools, and Amazon's mechanical turk", *Journal of Advertising Research*, Vol. 46 No. 1, pp. 141-155.

Kemper, T.D. (1966), "Representative roles and the legitimation of deviance", *Social Problems*, Vol. 13 No. 3, pp. 288-298.

Kianto, A., Andreeva, T. and Pavlov, Y. (2013), "The impact of intellectual capital management on company competitiveness and financial performance", *Knowledge Management Research & Practice*, Vol. 11 No. 2, pp. 112-122.

Klotz, A.C. and Buckley, M.R. (2013), "A historical perspective of counterproductive work behavior targeting the organization", *Journal of Management History*, Vol. 19 No. 1, pp. 114-132.

Knobe, J. (2003), "Intentional action and side effects in ordinary language", *Analysis*, Vol. 63 No. 3, pp. 190-194. No

Krippendorff, K. (1980), *Content Analysis: An Introduction to its Methodology*, Sage Publications, Beverly Hills, CA.

LaBar, K.S. and Cabeza, R. (2006), "Cognitive neuroscience of emotional memory", *Nature Reviews Neuroscience*, Vol. 7 No. 1, pp. 54-64.

LeBlanc, M.M. and Barling, J. (2005), "Understanding the many faces of workplace violence", in Fox, S. and Spector, P.E. (Eds), *Counterproductive Work Behavior: Investigations of Actors and Targets*, American Psychological Association, Washington, DC, pp. 41-63.

Lee, H., Kim, J.W. and Hackney, R. (2011), "Knowledge hoarding and user acceptance of online discussion board systems in eLearning: a case study", *Computers in Human Behavior*, Vol. 27 No. 4, pp. 1431-1437.

Lee, J. and Ok, C.M. (2014), "Understanding hotel employees' service sabotage: emotional labor perspective based on conservation of resources theory", *International Journal of Hospitality Management*, Vol. 36, pp. 176-187.

Lee, K.-H., McCann, D.P. and Ching, M. (2003), "Christ and business culture: a study of Christian executives in Hong Kong", *Journal of Business Ethics*, Vol. 43 Nos 1/2, pp. 103-110.

Lin, H.-F. (2015), "Linking knowledge management orientation to balanced scorecard outcomes", *Journal of Knowledge Management*, Vol. 19 No. 6, pp. 1224-1249.

Lin, T.-C. and Huang, C.-C. (2010), "Withholding effort in knowledge contribution: the role of social exchange and social cognitive on project teams", *Information & Management*, Vol. 47 No. 3, pp. 188-196.

McNeil, M. and Pedigo, K. (2001), "Western Australian managers tell their stories: ethical challenges in international business operations", *Journal of Business Ethics*, Vol. 30 No. 4, pp. 305-317.

Malik, O.F., Shahzad, A., Raziq, M.M., Khan, M.M., Yusaf, S. and Khan, A., (2018), "Perceptions of organizational politics, knowledge hiding, and employee creativity: the moderating role of professional commitment", *Personality and Individual Differences*, 142, pp. 232-237.

Martelo-Landroguez, S., Navarro, J.-G.C. and Cepeda-Carrión, G. (2019), "Uncontrolled counter-knowledge: its effects on knowledge management corridors", *Knowledge Management Research & Practice*, in-press.

Mathewson, S.B. (1931), *Restriction of Output among Unorganized Workers*, Viking Press, New York, NY.

Maylett, T. (2017), "How disengaged employees could be sabotaging your company's success", available at: www.decision-wise.com/how-disengaged-employees-could-be-sabotaging-your-companys-success/ (accessed 30 August 2017).

Meier, L.L. and Spector, P.E. (2013), "Reciprocal effects of work stressors and counterproductive work behavior: a five-wave longitudinal study", *Journal of Applied Psychology*, Vol. 98 No. 3, pp. 529-539.

Miles, M.B. and Huberman, A.M. (1994), *Qualitative Data Analysis: An Expanded Sourcebook*, Sage Publications, Thousand Oaks, CA.

Muldoon, J. (2012), "The Hawthorne legacy: a reassessment of the impact of the Hawthorne studies on management scholarship", *Journal of Management History*, Vol. 18 No. 1, pp. 105-119.

Myers, C.G. (2015), "Is your company encouraging employees to share what they know?", pp. 1-9, available at: https://hbr.org/2015/11/is-your-company-encouraging-employees-to-share-what-they-know (accessed 11 August 2017).

Neuman, J.H. and Baron, R.A. (2005), "Aggression in the workplace: a social-psychological perspective", in Fox, S. and Spector, P.E. (Eds), *Counterproductive Work Behavior: Investigations of Actors and Targets*, American Psychological Association, Washington, DC, pp. 13-40.

Nonaka, I. (1994), "A dynamic theory of organizational knowledge creation", *Organization Science*, Vol. 5 No. 1, pp. 14-37.

Orth, U. and Montada, L. (2006), "Feelings of revenge, retaliation motive, and posttraumatic stress reactions in crime victims", *Journal of Interpersonal Violence*, Vol. 21 No. 2, pp. 229-243.

Pan, W., Zhang, Q., Teo, T.S.H. and Lim, V.K.G. (2018), "The dark triad and knowledge hiding", *International Journal of Information Management*, Vol. 42, pp. 36-48.

Parmar, B.L., Keevil, A. and Wicks, A.C. (2017), "People and profits: the impact of corporate objectives on employees' need satisfaction at work", *Journal of Business Ethics*, Vol. 154 No. 1, pp. 1-21.

Paulin, D. and Suneson, K. (2012), "Knowledge transfer, knowledge sharing and knowledge barriers – three blurry terms in KM", *Electronic Journal of Knowledge Management*, Vol. 10 No. 1, pp. 81-91.

Pearson, C.M., Andersson, L.M. and Porath, C.L. (2005), "Workplace incivility", in Fox, S. and Spector, P. E. (Eds), *Counterproductive Work Behavior: Investigations of Actors and Targets*, American Psychological Association, Washington, DC, pp. 177-200.

Pilch, I. and Turska, E. (2015), "Relationships between Machiavellianism, organizational culture, and workplace bullying: emotional abuse from the target's and the perpetrator's perspective", *Journal of Business Ethics*, Vol. 128 No. 1, pp. 83-93.

Pratt, T.C., Cullen, F.T., Blevins, K.R., Daigle, L.E. and Madensen, T.D. (2006), "The empirical status of deterrence theory: a meta-analysis", in Cullen, F.T., Wright, J.P. and Blevins, K.R. (Eds), *Taking Stock: The Status of Criminological Theory*, Transaction Publishers, New Brunswick, New Jersey, pp. 367-395.

Rhee, Y.W. and Choi, J.N. (2017), "Knowledge management behavior and individual creativity: goal orientations as antecedents and in-group social status as moderating contingency", *Journal of Organizational Behavior*, Vol. 38 No. 6, pp. 813-832.

Riege, A. (2005), "Three-dozen knowledge-sharing barriers managers must consider", *Journal of Knowledge Management*, Vol. 9 No. 3, pp. 18-35.

Robinson, S.L. and Bennett, R.J. (1995), "A typology of deviant workplace behaviors: a multidimensional scaling study", *The Academy of Management Journal*, Vol. 38 No. 2, pp. 555-572.

Roethlisberger, F.J. and Dickson, W.J. (1956), *Management and the Worker: An account of a Research Program Conducted by the Western Electric Company, Hawthorne Works, Chicago*, Harvard University Press, Cambridge, MA.

Serenko, A. (2006), "The use of interface agents for email notification in critical incidents", *International Journal of Human-Computer Studies*, Vol. 64 No. 11, pp. 1084-1098.

Serenko, A. and Bontis, N. (2016), "Understanding counterproductive knowledge behavior: antecedents and consequences of intra-organizational knowledge hiding", *Journal of Knowledge Management*, Vol. 20 No. 6, pp. 1199-1224.

Serenko, A., Bontis, N. and Hardie, T. (2007), "Organizational size and knowledge flow: a proposed theoretical link", *Journal of Intellectual Capital*, Vol. 8 No. 4, pp. 610-627.

Serenko, A., Bontis, N. and Hull, E. (2016), "An application of the knowledge management maturity model: the case of credit unions", *Knowledge Management Research & Practice*, Vol. 14 No. 3, pp. 338-352.

Serenko, A. and Turel, O. (2010), "Rigor and relevance: the application of the critical incident technique to investigate email usage", *Journal of Organizational Computing and Electronic Commerce*, Vol. 20 No. 2, pp. 182-207.

Škerlavaj, M., Connelly, C.E., Cerne, M. and Dysvik, A. (2018), "Tell me if you can: time pressure, prosocial motivation, perspective taking, and knowledge hiding", *Journal of Knowledge Management*, Vol. 22 No. 7, pp. 1489-1509.

Small, M.W. and Cullen, J.L. (1995), "Socialization of business practitioners: learning to reflect on current business practices", *Journal of Business Ethics*, Vol. 14 No. 8, pp. 695-701.

Spector, P.E. and Fox, S. (Eds) (2005), "The stressor-emotion model of counterproductive work behavior", *Counterproductive Work Behavior: Investigations of Actors and Targets*, American Psychological Association, Washington, DC, pp. 151-174.

Spector, P.E. and Fox, S. (2010a), "Counterproductive work behavior and organisational citizenship behavior: are they opposite forms of active behavior?", *Applied Psychology*, Vol. 59 No. 1, pp. 21-39.

Spector, P.E. and Fox, S. (2010b), "Theorizing about the deviant citizen: an attributional explanation of the interplay of organizational citizenship and counterproductive work behavior", *Human Resource Management Review*, Vol. 20 No. 2, pp. 132-143.

Stach, A. and Serenko, A. (2009), "The impact of expectation disconfirmation on customer loyalty and recommendation behavior: investigating online travel and tourism services", *Journal of Information Technology Management*, Vol. 20 No. 3, pp. 26-41.

Taylor, F.W. (1911), *The Principles of Scientific Management*, Harper & Brothers Publishers, New York, NY.

Trusson, C., Hislop, D.W. and Doherty, N.F. (2017), "The rhetoric of 'knowledge hoarding': a research-based critique", *Journal of Knowledge Management*, Vol. 21 No. 6, pp. 1540-1558.

Tsay, C.H.-H., Lin, T.-C., Yoon, J. and Huang, C.-C. (2014), "Knowledge withholding intentions in teams: the roles of normative conformity, affective bonding, rational choice and social cognition", *Decision Support Systems*, Vol. 67 No. 11, pp. 53-65.

Ugrin, J.C. and Pearson, J.M. (2013), "The effects of sanctions and stigmas on cyberloafing", *Computers in Human Behavior*, Vol. 29 No. 3, pp. 812-820.

Urquhart, C., Light, A., Thomas, R., Barker, A., Yeoman, A., Cooper, J., Armstrong, C., Fenton, R., Lonsdale, R. and Spink, S. (2003), "Critical incident technique and explicitation interviewing in studies of information behavior", *Library & Information Science Research*, Vol. 25 No. 1, pp. 63-88.

Wallace, E. and de Chernatony, L. (2008), "Classifying, identifying and managing the service Brand saboteur", *The Service Industries Journal*, Vol. 28 No. 2, pp. 151-165.

Wang, K.-C., Hsieh, A.-T. and Huan, T.-C. (2000), "Critical service features in group package tour: an exploratory research", *Tourism Management*, Vol. 21 No. 2, pp. 177-189.

Wang, M., Liao, H., Zhan, Y. and Shi, J. (2011), "Daily customer mistreatment and employee sabotage against customers: examining emotion and resource perspectives", *Academy of Management Journal*, Vol. 54 No. 2, pp. 312-334.

Wang, Y.-S., Lin, H.-H., Li, C.-R. and Lin, S.-J. (2014), "What drives students' knowledge-withholding intention in management education? An empirical study in Taiwan", *Academy of Management Learning & Education*, Vol. 13 No. 4, pp. 547-568.

West, R. (2008), "The psychology of security", *Communications of the ACM*, Vol. 51 No. 4, pp. 34-40.

Williams, W. (1921), *What's on the Worker's Mind: By One Who Put on Overalls to Find out*, Charles Scribner's Sons, New York, NY.

Yahyapour, S., Shamizanjani, M. and Mosakhani, M. (2015), "A conceptual breakdown structure for knowledge management benefits using meta-synthesis method", *Journal of Knowledge Management*, Vol. 19 No. 6, pp. 1295-1309.

Zeelenberg, M. (1999), "The use of crying over spilled milk: a note on the rationality and functionality of regret", *Philosophical Psychology*, Vol. 12 No. 3, pp. 325-340.

Zhang, L. and Deng, Y. (2016), "Guanxi with supervisor and counterproductive work behavior: the mediating role of job satisfaction", *Journal of Business Ethics*, Vol. 134 No. 3, pp. 413-427.

Zhao, H. and Xia, Q. (2017), "An examination of the curvilinear relationship between workplace ostracism and knowledge hoarding", *Management Decision*, Vol. 55 No. 2, pp. 331-346.

Appendix. The questionnaire

Instructions: This survey presents four different situations that you might have come across in the workplace. Please answer the questions below about each of these situations.

Situation 1. Imagine the following situation. Your fellow colleague, manager, subordinate or employee *asked* you for information, advice, a document or a recommendation. You knew that it was *extremely important* to him/her, and that he/she would be able to productively *apply* it to his/her work. However, you *deliberately* provided him/her with the *wrong* information, advice, document or recommendation despite having/knowing the correct one.

Situation 2. Imagine the following situation. You realized that your fellow colleague, manager, subordinate or employee needed information, advice, a document or a recommendation, but he/she *did not request it* from you. You knew that it was *extremely important* to him/her, and that he/she would be able to productively *apply* it to his/her work. However, you *deliberately* provided him/her with the *wrong* information, advice, document or recommendation despite having/knowing the correct one.

Situation 3. Imagine the following situation. Your fellow colleague, manager, subordinate, or employee *asked* you for information, advice, a document or a recommendation. You knew that it was *extremely important* to him/her, and that he/she would be able to productively *apply* it to his/her work. However, you *deliberately* failed to provide him/her with this information, advice, document or recommendation despite having/knowing it.

Situation 4. Imagine the following situation. You realized that your fellow colleague, manager, subordinate, or employee needed information, advice, a document or a recommendation, but he/she *did not request it* from you. You knew that it was *extremely important* to him/her, and that he/she would be able to productively *apply* it to his/her work. However, you *deliberately* failed to provide him/her with this information, advice, document, or recommendation despite having/knowing it.

Questions about each situation:

During your entire working career, how many times have you experienced a situation similar to the one described above? (from "never" to "over 20").

Out of all situations similar to the situation described above, recall the one that had the most dramatic impact on you, your organization, or the person asking for assistance (i.e. it was the most critical). (If you have never experienced a similar situation, proceed to Situations 2, 3, 4 or demographics (the text was adjusted for each situation)):

- Explain in detail what happened. (open-ended)
- Did you act against a particular individual or the entire organization? (open-ended)
- Why did you do that? (open-ended)
- What impact did it have on this individual and/or this organization? (open-ended)
- Did you ever regret your action? (options: yes; no; not sure/never thought about it)

About the author

Dr Alexander Serenko is a Visiting Professor in the Faculty of Information, the University of Toronto, Canada and a Full Professor of Management Information Systems in the Faculty of Business Administration at Lakehead University, Canada. Dr Serenko holds a PhD in Management Information Systems from McMaster University. His research interests pertain to scientometrics, knowledge management, and technology addiction. Alexander has published more than 80 articles in refereed journals, including *MIS Quarterly*, *European Journal of Information Systems*, *Information & Management*, *Communications of the ACM* and *Journal of Knowledge Management*. He has also won six Best Paper awards at Canadian and international conferences. In 2015, Dr Serenko received the Distinguished Researcher Award which is the highest honor conferred by Lakehead University for research and scholarly activity. Alexander Serenko can be contacted at: a.serenko@utoronto.ca