Knowledge sabotage as an extreme form of counterproductive knowledge behavior: the perspective of the target

Alexander Serenko

Abstract

Purpose – *This study aims to explore the existence of knowledge sabotage in the contemporary organization from the perspective of the target.*

Design/methodology/approach – *This study collected and analyzed 172 critical incidents reported by 109 employees who were targets of knowledge sabotage in their organizations.*

Findings – *Over 50 per cent of employees experienced at least one knowledge sabotage incident. Knowledge sabotage is driven by three factors, namely, gratification, retaliation against other employees and one's malevolent personality. Knowledge saboteurs are more likely to provide intangible than tangible knowledge. Knowledge sabotage results in extremely negative consequences for individuals, organizations and third parties. Organizations often indirectly facilitate knowledge sabotage among their employees. Both knowledge saboteurs and their targets believe in their innocence – saboteurs are certain that their action was a necessary response to targets' inappropriate workplace behavior, whereas targets insist on their innocence and hold saboteurs solely responsible.*

Practical implications – *Organizations should recruit employees with compatible personalities and working styles, introduce inter-employee conflict prevention and resolution procedures, develop anti-knowledge sabotage policies, clearly articulate the individual and organizational consequences of knowledge sabotage and eliminate zero-sum game-based incentives and rewards.*

Originality/value – *This is the first study documenting knowledge sabotage from the target's perspective.*

Keywords *Knowledge sabotage, Counterproductive workplace behavior, Critical incident technique, Target, Victim, Knowledge sharing*

Paper type *Research paper*

Alexander Serenko is based at the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Canada.

1. Introduction

As soon as the first knowledge management (KM) concepts entered the mainstream academic research, scholars became highly interested in the development of productive KM practices and mechanisms and, particularly, in knowledge sharing. Gradually, the scope of their inquiry has embraced various counterproductive knowledge behaviors representing the "dark side of KM" (Alter, 2006). For example, a search of the ABI/INFORM Collection on the phrase "knowledge hiding" in books, conference proceedings and scholarly articles revealed that the first documented knowledge hiding publications appeared around 2011 and the volume of related works has skyrocketed since 2015. The extant literature presents six categories 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 (Trusson *et al.*, 2017), counter-knowledge sharing (Cegarra-Navarro *et al.*, 2015; Martelo-Landroguez *et al.*, 2019) and knowledge hiding (Connelly *et al.*, 2012; Škerlavaj *et al.*, 2018; Hernaus *et al.*, 2019) – each of which differs in terms of its negative impact on

Received 29 June 2019
Revised 30 December 2019
Accepted 26 February 2020

an organization. Recently, Serenko (2019) empirically demonstrated the existence of knowledge sabotage as an extreme form of counterproductive knowledge behavior by collecting and analyzing 177 knowledge sabotage incidents reported by 100 knowledge saboteurs (i.e. perpetrators) and showed that it is conceptually different from the other forms of counterproductive knowledge behavior. The results revealed the presence of knowledge sabotage in the contemporary organization, which makes it the seventh type of counterproductive knowledge behavior.

Knowledge sabotage occurs when an employee deliberately provides incorrect knowledge to his or her fellow employee or conceals highly critical knowledge while being aware that this knowledge is needed and must be productively applied in the workplace. In all cases, the saboteur possesses the required knowledge and is aware of the target's need for knowledge. The use of wrong knowledge or the inability to apply the required knowledge may produce truly devastating consequences for this employee, the entire organization and even third parties (Serenko, 2019). For instance, individuals may be wrongfully reprimanded, publicly humiliated or unjustly dismissed. Work duplication and wasted effort produce inefficiencies. Terminated and delayed projects not only result in financial expenses and lost image but also impact customers. Knowledge sabotage, as a form of unethical behavior, may cause unnecessary stress and reduce employees' well-being, thereby negatively impacting their productivity (Giacalone and Promislo, 2010). Moreover, this may affect not only knowledge sabotage victims but also its witnesses (Totterdell *et al.*, 2012). Observers of unethical workplace behavior often copy the perpetrators' behavior (Reich and Hershcovis, 2015), which suggests that knowledge sabotage witnesses may later propagate it throughout the entire organization. The presence of knowledge sabotage affects an overall image of an organization and may result in negative publicity, thereby reducing its chances for attracting and retaining the best human capital. The arguments above demonstrate that the notion of knowledge sabotage is worth further study.

Particularly, it is vital to understand the knowledge sabotage phenomenon from the target's point of view. Knowledge sabotage involves a dyadic saboteur-target relationship and exploring the phenomenon from the perspective of a single party may offer an incomplete perspective (Bozeman and Hershcovis, 2015). For example, knowledge sabotage perpetrators may not be fully aware of the consequences of their actions on the victim's emotional state (e.g. reduced job satisfaction) and subsequent behavioral changes (e.g. lower productivity). Knowledge saboteurs argue that, in many cases, they were provoked by the target's hostile, unhelpful and unproductive behavior (Serenko, 2019). However, do their targets share the same point of view? What impact does knowledge sabotage have on them? Whom do they hold responsible? Do they change their attitude and/or behavior toward saboteurs and/or their organizations? Do they retaliate against the perpetrators by the same means? Do they report knowledge sabotage incidents and, if so, what happens afterward? The present study attempts to answer these questions.

In addition, when participating in knowledge sabotage research studies, saboteurs may exhibit a stronger social desirability bias than their targets. Social desirability bias is a conscious or subconscious tendency of study participants to respond to questions in a manner, which is viewed favorably by others. As a result, they may exaggerate their positive behaviors and under-report negative ones (Crowne and Marlowe, 1960; Podsakoff *et al.*, 2003; Kwak *et al.*, 2019). Because knowledge sabotage represents an extreme form of counterproductive knowledge behavior, it is sensitive to social desirability bias. For instance, some saboteurs may understate the frequency or magnitude of such behavior or report only somewhat trivial offences while concealing the truly devastating ones. In contrast, knowledge sabotage victims are less likely to be susceptible to social desirability bias and should report a more realistic description of the issue. Moreover, by comparing and contrasting the different perspectives of perpetrators and their victims, it may be possible to develop a better comprehension of the issue and generate new insights. By

looking at the holistic perspective offered by both parties, it may be possible to construct an integrated framework of knowledge sabotage behavior resulting in novel theoretical insights and useful practical implications. Thus, the present study continues the line of inquiry established by Serenko (2019), who focused on knowledge saboteurs, and explores the notion of knowledge sabotage in the contemporary workplace from the target's perspective.

Particularly, by using the critical incident technique (CIT) (Flanagan, 1954), this study collected and analyzed 172 critical incidents from 109 employees who were victims of knowledge sabotage in their organizations. The findings confirmed that knowledge sabotage is widespread in the contemporary organization. Such counterproductive behavior may impede intra-organizational knowledge flows and result in deleterious consequences for employees, organizations and even third parties. Knowledge sabotage rarely takes a form of revenge against one's organization; instead, it is driven by personal gratification, a desire to retaliate against fellow employees and one's malevolent personality. Both knowledge saboteurs and their targets maintain their innocence – saboteurs believe that their action was a necessary, provoked response to a targets' inappropriate behavior, whereas targets hold saboteurs solely responsible.

The rest of this article is structured as follows. Section 2 forms a conceptual foundation for this study and reviews prior works. Section 3 outlines this study's methodology and Section 4 presents the findings. Section 5 discusses the theoretical and practical implications, and finally, Section 6 concludes the study.

2. Literature review

The purpose of this section is three-fold. The first is to discuss the extant literature on the topic of counterproductive workplace behavior to justify the significance of this issue and show a need for further research. The second goal is to present the concept of knowledge sabotage and briefly cover its conceptual definition, outline its typology and demonstrate that it is different from the other forms of counterproductive knowledge behaviors. The third objective is to emphasize a need to explore the phenomenon from the perspective of knowledge of sabotage victims.

2.1 Counterproductive workplace behavior

Exchange theories (Blau, 1964) and employee-organization relationship frameworks (Tsui *et al.*, 1997) posit that employees and employers engage in a certain form of economic and/or social exchange where the former receives something of value and, in return, provides the latter with certain contributions in the form of labor and knowledge. Thus, under the condition of fair exchange, it behooves employees to properly perform their specific duties and contribute to the overall organizational objective. Evidence, however, reveals that, regardless of the actual and/or perceived fairness of employee-organization exchange, workers frequently engage in various counterproductive behaviors, defined as intentional acts that harm or intend to harm organizations and/or their stakeholders (Robinson and Bennett, 1995; Spector and Fox, 2005). Of particular interest are counterproductive behaviors targeted at other organizational members because such undesirable actions are highly relevant in the context of the contemporary knowledge organization.

The extant literature has identified a variety of such counterproductive behaviors ranging from relatively minor nuisances to major, illegal acts that have drastic effects on other employees and, by extension, on entire organizations. For example, *social undermining* is an ongoing behavior intended to impede someone's ability to develop and maintain healthy interpersonal relationships, success and a favorable reputation (Duffy *et al.*, 2002). *Workplace rudeness* is a covert form of abuse when perpetrators formally hide their malevolent motives when they publicly interrupt, ignore, insult or reprimand other employees (Johnson and Indvik, 2001). *Emotional abuse* represents hostile verbal and non-

verbal behavior that is directed at gaining compliance from others when abusers yell, scream, use derogatory names, make aggressive eye contact and ridicule their victims (Keashly and Harvey, 2005). *Workplace incivility* (Blau and Andersson, 2005; Pearson *et al.*, 2005) is a "low-intensity deviant behavior with ambiguous intent to harm the target, in violation of workplace norms for mutual respect" (Andersson and Pearson, 1999, p. 457), which is frequently present in the organizational environment. *Workplace bullying or mobbing* (Vartia, 2001; Harvey *et al.*, 2009; Bartlett and Bartlett, 2011) happens when employees continually experience oppressive and annoying behavior, which they cannot easily ignore, dismiss or terminate. Examples include gossiping, laughter, slander and scorning. *Workplace discrimination, abuse, aggression, harassment, and violence* represent illicit acts that drastically affect the target's emotional and/or physical well-being (LeBlanc and Barling, 2005; Neuman and Baron, 2005; Krieger *et al.*, 2006). In response to such behaviors, victims develop various coping strategies, including support seeking, detachment and avoiding interactions with the instigator (Cortina and Magley, 2009).

The lines between the counterproductive behaviors above are blurred and one behavior frequently incorporates some attributes of the others (Hershcovis, 2011). For example, workplace bullying may include some characteristics of workplace rudeness, emotional abuse and social undermining – all directed at a particular individual with a specific malevolent goal in mind. Nevertheless, all of these actions are directed at other fellow employees, including managers, colleagues and subordinates.

On the one hand, an inquiry into the nature of counterproductive workplace behaviors has helped researchers better comprehend inter-employee relationships and develop proactive approaches to reduce the amount of harm inflicted upon employees, their organizations and other stakeholders. On the other hand, Serenko (2019) recently demonstrated that the list of counterproductive workplace behaviors above is far from complete and may be extended further.

2.2 Knowledge sabotage

The literature posits that, in addition to the counterproductive workplace behaviors discussed in the previous sub-section, to achieve their ego-driven or malicious goal, perpetrators often engage in workplace sabotage, defined as conscious, intentional and malevolent acts that harm other organizational members or stakeholders (Crino, 1994; Spector and Fox, 2005; Klotz and Buckley, 2013). Particularly, they may engage in knowledge sabotage, which is the most extreme form of counterproductive knowledge behavior. According to Serenko (2019, p. 1264), knowledge sabotage is defined as follows:

> [...] 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: 1) the saboteur acts intentionally (intention); 2) the saboteur is fully aware of the target's need for knowledge (need awareness); 3) the saboteur possesses the required knowledge (knowledge possession); 4) the required knowledge is extremely important to the target (knowledge importance); 5) the saboteur is aware of the knowledge's importance to the target (knowledge importance awareness); and 6) the saboteur is aware that the target would be able to productively apply the required knowledge to work-related tasks (knowledge application).

The previous attempt to explore and document the knowledge sabotage phenomenon by Serenko (2019) unexpectedly revealed that almost all knowledge saboteurs act against other employees rather than against their organizations and that a majority of incidents are caused by interpersonal conflict and competition between knowledge saboteurs and their targets. Knowledge sabotage is the means by which employees engage in retaliation caused by the target's hostile behavior, inability to help others and sub-standard performance. Some employees also engage in knowledge sabotage because they believe

that they compete with the targets for something of value, for example, a lucrative customer or a promotion. As such, saboteurs are convinced that their targets have previously shown disruptive behavior, treated them and/or other employees unfairly and engaged in knowledge sabotage themselves. Saboteurs consider their targets lazy, ignorant, uncooperative, unproductive and incompetent workers deserving a proper punishment. For them, knowledge sabotage is the means by which they teach a lesson to someone or achieve a particular egoistic goal at the expense of their organization. Most saboteurs are able to achieve their goal – their victims are formally reprimanded, publicly humiliated and even wrongfully terminated. Saboteurs often get promotions, successfully eliminate internal competition and secure other tangible rewards. Their targets, however, waste time completing unnecessary tasks, re-doing their work and duplicating knowledge, which reduces their efficiency and reflects poorly on their performance appraisal. At the same time, their entire organization incurs financial losses because it has to finance the inefficiencies and cover all expenses associated with knowledge sabotage. For example, organizations have to incur extra hiring and training expenses when knowledge sabotage victims are wrongfully terminated. However, almost never do saboteurs envision or assess the long-term consequences of their malevolent actions.

The typology of knowledge sabotage is presented in the form of a two by two matrix along the following dimensions:

1. Provoked (when the target requested knowledge from the saboteur) vs unprovoked (when the target did not request knowledge from the saboteur).
2. Active (when the saboteur provided wrong knowledge) vs passive (when the saboteur concealed critical knowledge).

The passive form of knowledge sabotage is more popular than an active one. This happens because first, actively acting against someone requires more cognitive resources than passively ignoring their need for knowledge and watching them struggle. Second, active knowledge sabotage also necessitates the fabrication of wrong knowledge, whereas passive does not and is, therefore, much easier to engage in. Third, in cases of active knowledge sabotage, victims may eventually track the wrong knowledge back to the saboteur and formally complain to a manager, which may lead to some form of disciplinary action. In contrast, this scenario is highly unlikely in cases of passive knowledge sabotage.

Knowledge sabotage is conceptually different from the other forms of 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 (Trusson *et al.*, 2017), counter-knowledge sharing (Cegarra-Navarro *et al.*, 2015; Martelo-Landroguez *et al.*, 2019) and knowledge hiding (Connelly *et al.*, 2012; Škerlavaj *et al.*, 2018; Hernaus *et al.*, 2019). First, those who engage in knowledge sabotage deliberately and consciously act against their organization or its employees; whereas they may not fully realize the entire range of unanticipated long-term consequences of their actions, their malicious intent is clear from the very beginning. In contrast, the malicious intention may not be present in some other forms of counterproductive knowledge behavior. For example, employees may share unconfirmed, gossip-based knowledge (i.e. engage in counter-knowledge sharing) merely out of boredom. Second, a knowledge saboteur always possesses the required knowledge yet abuses this situation, whereas those who are disengaged from or ignorant of knowledge sharing may not have the required knowledge in their possession. Third, a knowledge saboteur is fully aware of the target's need for knowledge, the high value of this knowledge and the target's ability to productively apply this knowledge to work-related tasks. In contrast, employees who hoard knowledge or who only partially share their knowledge may not necessarily realize so. Fourth, in contrast to knowledge hiding, which is accompanied by an unambiguous

request to share knowledge, in cases of unprovoked knowledge sabotage, knowledge saboteurs may themselves initiate their destructive behavior against an unsuspecting victim. It is for these reasons, out of all types of counterproductive knowledge behaviors, knowledge sabotage has the strongest negative impact on an organization and its internal (shareholders and employees) and external (customers) stakeholders. For a detailed conceptualization and typology of knowledge sabotage, please refer to Serenko (2019).

2.3 The perspective of the target

Despite the novelty and contribution of the previous knowledge sabotage investigation, it presented an incomplete picture of this important phenomenon because it focused on the perspective of knowledge saboteurs only. At the same time, it is possible that knowledge sabotage targets – those who became victims of their managers, colleagues or subordinates – may offer a different opinion, which may extend or even alter our understanding of knowledge sabotage in the context of the contemporary organization. For example, by developing a model of workplace harassment from the victim's perspective, Bowling and Beehr (2006) identified a number of unique environmental, organizational and individual factors explicating the phenomenon, as well as its antecedents and consequences. At the same time, this was impossible to achieve by focusing on perpetrators only. Thus, the present study analyzes the phenomenon from the target's viewpoint.

As the previous study revealed (Serenko, 2019), from the perspective of knowledge saboteurs, knowledge sabotage is mainly triggered by two factors:

1. Interpersonal conflict between employees due to personal incompatibility and disagreement.
2. Competition over extrinsic rewards such as promotion and monetary benefits.

The literature suggests that workplace conflict, defined as a situation when employees believe that their goals or interests are in opposition to one another (De Dreu and Gelfand, 2008), has traditionally been an irrevocable part of inter-employee relationships. Workplace conflict can be classified as task conflict when group members disagree on the way their team is doing its job (e.g. how to perform a particular job-related activity) and relationship conflict, when employees differ in their values, norms, beliefs, aspirations, expectations about one another, etc (e.g. interpersonal incompatibilities among employees) (Jehn, 1995). Task-related conflict may have either a negative or positive impact on employee performance, whereas relationship-related conflict always produces a negative outcome (De Dreu, 2008).

Another reason why employees engage in knowledge sabotage is a perceived competition over extrinsic rewards. The theory of cooperation and competition (Deutsch, 1973, 2012) posits that, when employees perceive that by collaborating with others they increase their own and others' chances for attaining their goals, they act in a cooperative manner and exhibit positive behavior for the benefit of everyone involved. In contrast, when employees perceive that they have to compete for scarce rewards (i.e. zero-sum game), they perceive conflict and act in a competitive manner by trying to increase their own chances of attaining their goal at the expense of the others. As a result, they may engage in counterproductive behavior including knowledge sabotage.

During active knowledge sabotage episodes, employees engage in a specific form of workplace deception when lying to their managers, colleagues and subordinates. Regrettably, lying has become prevalent in the contemporary business environment in both for-profit and non-profit organizations of all sizes (Shulman, 2008). Employees deceive others to inflate their performance ranking, evade difficult tasks, obtain unearned rewards,

avoid punishment, appease others, cover up mistakes, appear knowledgeable and justify tardiness or absence (Payne, 2008; Indvik and Johnson, 2009). In some situations, employees lie to harm other organizational members (Indvik and Johnson, 2009). In the knowledge sabotage context, it is argued that, when interpersonal conflict and/or zero-sum based competition arise, saboteurs use deception as a tool to punish, retaliate against and/or take advantage of other employees or in rare cases, their entire organizations by means of knowledge sabotage. The previous study (Serenko, 2019) has shed some light on this issue from the perspective of knowledge saboteurs. However, as argued earlier, this approach may offer an incomplete or even somewhat biased, description of the phenomenon. The present study attempts to expand our understanding of this critical issue and empirically explore the topic of knowledge sabotage from the perspective of the target.

3. Methodology

3.1 The methodological approach

The CIT (Flanagan, 1954) was used for data collection and analysis. The CIT may be best described as a set of general and flexible guidelines for documenting the extreme episodes of human behavior within a particular domain to make inferences, build theory and develop practical recommendations (Butterfield *et al.*, 2005; Serenko, 2006; Serenko and Turel, 2010). It was developed and documented by Colonel John C. Flanagan during his work in the aviation psychology program of the US Air Force. According to the CIT, 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. 357). The incident is considered critical if it has a significant impact on the person's ability to complete (or fail) an important task (Andersson and Nilsson, 1964). As a result, such critical incidents are retained in people's long-term memory for very long periods of time and individuals may reliably self-report these episodes when prompted by the researchers (Koenemann-Belliveau *et al.*, 1994). One of the key advantages of this technique is its flexibility because it allows researchers to collect and analyze virtually any attributes of the incidents that are deemed relevant in the context of the study. As such, the CIT represents the collection and analysis of brief factual reports of people's actions in response to explicit situations or problems caused by various environmental factors, including other people's behavior (e.g. knowledge sabotage). Similar to other qualitative data analysis techniques, the CIT is considered a valid and reliable method capable of producing generalizable findings in virtually all areas of human activity (Andersson and Nilsson, 1964; Ronan and Latham, 1974).

The CIT is suitable in the context of the present study for the following reasons. *First*, the application of the CIT ensures an accurate comparison of this study's findings with those reported by Serenko (2019). *Second*, being a victim of a knowledge sabotage incident represents an extreme form of negative behavior, which stays in the person's long-term memory and may be easily recalled. *Third*, knowledge sabotage is a form of unethical behavior, which may be identified with the application of the CIT (Small and Cullen, 1995; McNeil and Pedigo, 2001; Byrne *et al.*, 2014). *Fourth*, the CIT may be successfully used in self-administered surveys with both open- and closed-ended questions.

The present study considers instances of an active type of knowledge sabotage only. When looking at the provoked-passive type of knowledge sabotage from the target's perspective (i.e. when the saboteur concealed critical knowledge when it was requested), it is difficult to reliably identify provoked-passive knowledge sabotage incidents because the target may not be absolutely sure whether the saboteur acted intentionally and/or actually possessed the required knowledge. With respect to the unprovoked-passive type of knowledge sabotage (i.e. when the saboteur concealed critical knowledge when it was not requested), the target may never be sure whether the saboteur was fully aware of the target's need for knowledge, whether this knowledge was extremely important to the target, whether the target was able to apply this knowledge and whether the saboteur actually possessed the

required knowledge. As such, many passive knowledge sabotage incidents may remain unknown to the targets even though they took place in their organization. In contrast, all employees are well aware of and remember all incidents when they became the targets of active knowledge sabotage (i.e. when they were provided with wrong, critical knowledge). Thus, consistent with the basic CIT principles, respondents were asked to recall and describe very memorable episodes when they became victims of knowledge sabotage in their workplace.

3.2 The research instrument

The research instrument presented two situations, which were developed by adapting the instrument of Serenko (2019) and by relying on a definition of knowledge sabotage (Appendix 1). Because this study focuses on knowledge sabotage targets (i.e. victims), the situations and questions were modified accordingly. The pre-screening instrument asked respondents about the number of years of full-time work experience, presented the two situations in random order and asked whether they had experienced a similar situation. A compensation of US$0.05 was offered for the completion of the pre-screening survey. The full-study instrument also contained the same two situations presented in random order, which were accompanied by 10 questions pertaining to:

1. Incident description.
2. Intended victim.
3. Driver of the behavior.
4. Impact.
5. Attitude change toward the saboteur.
6. Attitude change toward the organization.
7. Retaliatory behavior.
8. Attribution of responsibility.
9. Occurrence frequency.
10. Incident reporting and its outcome.

Basic demographic data were also collected. This project was described as a neutral knowledge sharing study and the word "sabotage" was never mentioned. Those who completed the full-study instrument were offered compensation of US$2.00.

3.3 Respondents and recruitment

Respondents were recruited from Amazon's Mechanical Turk (mTurk), which serves as an online marketplace employing over 500,000 independent workers performing various human intelligence tasks including participation in research projects. In the context of the present study, mTurk was an excellent data collection environment for the following reasons. *First*, becoming a victim of knowledge sabotage is a somewhat embarrassing experience and accurately reporting it requires a full degree of anonymity. When using mTurk, researchers see only the respondent's worker ID and no personal information such as name or e-mail address is exchanged. In addition, the survey did not solicit any personally identifiable information. *Second*, only those who had at least two years of full-time work experience, resided in the USA and experienced at least one knowledge sabotage incident were allowed to participate in the full study. For this, mTurk provides various options to pre-screen the candidates. *Third*, compared to subjects recruited randomly online or university students, mTurk participants are more geographically diverse, which

improves results generalizability (Buhrmester *et al.*, 2011). *Fourth*, mTurk workers are highly motivated because requesters (i.e. researchers) may reject their work if they are unsatisfied with its quality – which may negatively affect the workers' ranking scores and prevent them from participating in the future mTurk activities. As a result, findings generated based on mTurk data sets are consistent with those reported previously (Berinsky *et al.*, 2012; Goodman *et al.*, 2012; Kees *et al.*, 2017). *Fifth*, mTurk allows researchers to recruit only very reliable participants. In the present study, the following requirements were established:

- Human intelligence task (HIT) approval rate = 96 per cent;
- Location = The USA; and
- The number of HITs approved = 1,000.

Last, mTurk may be successfully used with a variety of data collection approaches including the CIT (Landers and Callan, 2014).

3.4 Data analysis

Qualitative data analysis of the open-ended responses was done (Miles and Huberman, 1994). A draft codebook was initially developed based on the previous findings of Serenko (2019). As the coding process progressed, the codes were continuously modified, merged and removed – and brand new codes were introduced as needed. The final round of coding was done by two independent coders who had advanced doctoral-level training in qualitative research. All differences were identified and re-analyzed until a mutual agreement was reached. An acceptable level of inter-rater agreement was obtained (the Krippendorff's (1980) agreement coefficient exceeded 0.8). As recommended by Ferraris *et al.* (2019), the first- and second-level codes were summarized in an easy-to-comprehend format (Appendix 2). In all applicable cases, each theme was also coded whether the code was present or absent. For example, when coding the impact of the incident on the target, the organization and/or the third party, it was first established whether the impact took place – some respondents stated that the incident had an impact, whereas others said that it did not.

4. Results

4.1 Overview

Out of 324 respondents who filled in the pre-screening survey, 54 per cent indicated that they had been a target of a knowledge sabotage incident at least once and 45 per cent had experienced it multiple times. In total, 176 full-study invitations were sent and 109 completed surveys were received at the response rate of 62 per cent. Overall, 172 critical incidents were reported and used in the analysis. In total, 100 per cent of the respondents described an incident of a provoked type of knowledge sabotage. Out of them, 58 per cent (i.e. 63 individuals) also reported an unprovoked knowledge sabotage incident. Over half of the respondents said they experienced a similar incident multiple times.

In total, 59 per cent of the respondents were women. They had 16 years of full-time work experience, on average, ranging from 2 to 40 years. Their average age was 37 years old, ranging from 23 to 66 years old. In terms of their education, 14 per cent had high school or less, 33 per cent had an associate degree (a two-year degree) or some college, 38 per cent had a bachelor's degree, 13 per cent had a master's degree and 2 per cent had a Ph.D.

4.2 Saboteurs and the type of knowledge

Table I describes the characteristics of saboteurs and the type of wrong knowledge provided. A majority of all knowledge sabotage incidents were generated by colleagues, some by managers and a few by subordinates. Most of them offered wrong intangible

Table I Characteristics of saboteurs and provided knowledge

	Provoked type	*Unprovoked type*
Saboteur	The colleague – 69% The manager – 18% The subordinate – 7% Other/unclear – 6%	The colleague – 68% The manager – 24% The subordinate – 3% Other/unclear – 5%
Type of wrong knowledge	Intangible – 69% Tangible – 28% Other/unclear – 3%	Intangible – 81% Tangible – 16% Other/unclear – 3%

knowledge such as verbal advice, recommendations or tips. Some provided wrong tangible knowledge, including training manuals, computer files, documentation, reports, notes and templates. Saboteurs who engaged in an unprovoked type of knowledge sabotage were more likely to provide intangible knowledge. No other relationships between the type of saboteurs and the type of provided knowledge were observed.

The quotes below describe the experience of knowledge sabotage targets:

> P19. "I was doing the remodel on a store in an overnight leader position. I needed the floor plans from a similar location to copy and asked someone else [a colleague] to bring me them. They had recently been updated and I knew they had the copy in the office [. . .] They purposefully gave me the wrong ones. You know how I know? They kinda smirked when I figured it out after setting up several aisles wrong." (Provoked; tangible knowledge provided by a colleague)

> P40. "It was actually a subordinate of mine who disliked me greatly and had befriended my boss and created a relationship with her that excluded me. I asked her for some information about appointments coming up and if people had confirmed and she said she had no knowledge of people confirming. Later I checked my calendar and realized people had confirmed and I was now going to be late. When I questioned her about it my boss overheard and listened to her answer which was her saying she told me that she would put all confirmations on my calendar and I should check, not that she had no knowledge of people confirming. She flat out lied, but my boss believed her despite my over 10 years with the company." (Provoked; intangible knowledge provided by a subordinate)

> P102. "My former manager told me that there were some forms that needed to be typed up for their client. I didn't request it, but she came to me and told me that it needed to be complete[d] and that it was important for me to do it since I did a lot of data entry. I found out later that day that the information she gave me were the wrong reports and that I ended up wasting my afternoon typing report that wasn't even right." (Unprovoked; intangible knowledge provided by a manager)

Figures 1 and 2 show that, on average, knowledge sabotage incidents took place rarely. In about 10 per cent of organizations, knowledge sabotage was an unfortunate exception. However, in around 7 per cent of organizations, knowledge sabotage happened often or very often.

4.3 Targets

Over 70 per cent of the saboteurs had a single target in mind – an individual such as a colleague, a subordinate or a manager (Table II). Very few saboteurs acted solely against their organization. In cases of multiple targets, most acted against an individual and their organization simultaneously. Overall, these findings are similar to the ones reported in the previous investigation (Serenko, 2019), which also concluded that a majority of all knowledge sabotage incidents are aimed at another individual – typically, a colleague.

Figure 1 The frequency of occurrence – provoked knowledge sabotage incidents

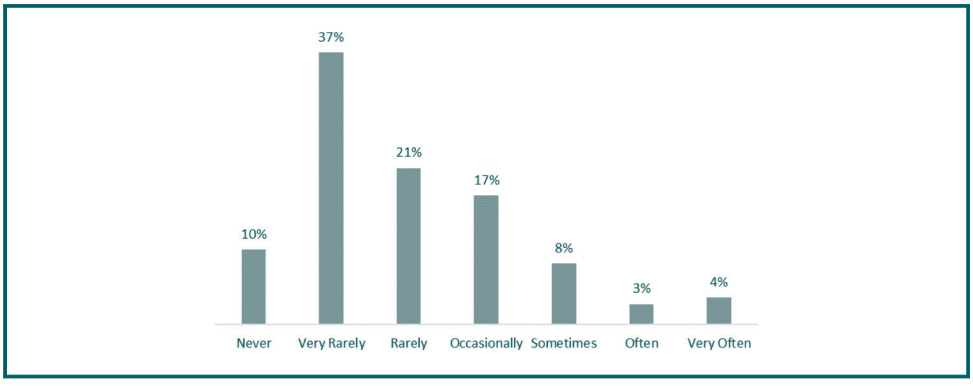


Figure 2 The frequency of occurrence – unprovoked knowledge sabotage incidents

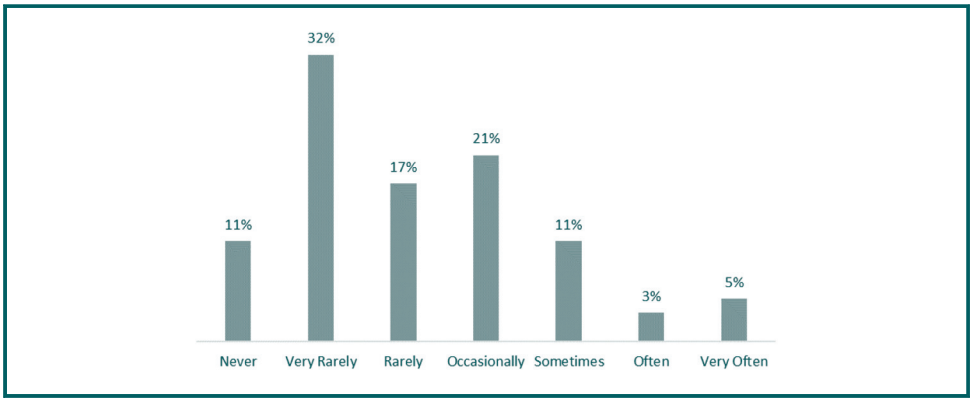


Table II Targets

Provoked type	*Unprovoked type*
Single target – 71% – The individual – 66% – The organization – 4% – The third party – 1% Multiple targets – 29% – The individual and the organization – 23% – The individual, the organization and the third party – 5% – The organization and the third party – 1%	Single target – 76% – The individual – 70% – The organization – 5% – The third party – 1% Multiple targets – 24% – The individual and the organization – 14% – The individual and the third party – 5% – The individual, the organization and the third party – 5%

4.4 Knowledge sabotage drivers

Table III lists a number of factors driving saboteurs' behavior. Three general categories of drivers emerged:

1. Gratification.
2. Retaliation against other employees.
3. Malevolent personality.

Table III Motivation

Provoked type	*Unprovoked type*
Gratification – 33%	Gratification – 37%
– Personal career – 18%	– Personal career – 18%
– Personal gain – 13%	– Personal gain – 17%
– Mistake cover up – 2%	– Mistake cover up – 2%
Retaliation tendency – 29%	Retaliation tendency – 29%
– Envy – 12%	– Personal incompatibility – 19%
– Grudge – 10%	– Envy – 7%
– Personal incompatibility – 7%	– Grudge – 3%
Malevolent personality – 29%	Malevolent personality – 27%
– Malevolence toward others – 11%	– Malevolence toward others – 13%
– Poor attitude – 11%	– Playing jokes on others – 10%
– Playing jokes on others – 5%	– Poor attitude – 2%
– Psychological issues – 2%	– Psychological issues – 2%
Organization-related – 4%	Organization-related – 0%
– Money-saving – 4%	
Other – 5%	Other – 7%

These motives were approximately equal in terms of their magnitude.

First, *gratification drivers* included personal career advancement (when saboteurs tried to get the target in trouble, denied a promotion, demoted or wrongfully dismissed because they wanted the target's position), personal gain (when saboteurs wanted a monetary reward, a lucrative client or something of value that otherwise might have been allocated to the target) and covering up previous mistakes (when saboteurs tried to attribute the cause of a previous mistake to the target or another third party). Interestingly, in career and personal gain-related cases, saboteurs often believed that they were wrongly denied a position or a reward that they presumably deserved – for example,

> P86. "I think she wanted my job. I think she felt that she was deserving of it so she tried to sabotage me." (Personal Career)
>
> P100. "They wanted me fired and wanted the client for themselves." (Personal Gain)
>
> P95. "[. . .] to prevent her shift from being looked as one that it [the problem] occurred on." (Mistake Cover up)

Second, saboteurs tried to *retaliate against other employees* because of irreconcilable differences between their personalities, which made saboteurs experience negative emotions toward targets and a desire to punish them. A tendency to retaliate was also caused by a grudge from a prior conflict between the parties and saboteurs tried to avenge themselves by means of knowledge sabotage. Another interesting retaliation motive resulted from saboteurs' envy of targets' professional success and they chose to engage in questionable behavior to impede it. A key difference between gratification- and retaliation-driven factors is that, in case of the former, saboteurs intended to receive some form of a tangible reward or to prevent punishment, whereas, in case of the latter, saboteurs' sole goal was to inflict harm upon their targets. For example,

> P91. "We haven't ever gotten along very well, so I believe it is just another one of her nasty tactics." (Personal Incompatibility)
>
> P4. "I think it had to do with me making a joke during a time at lunch which he got really mad about and he was mad at me ever since." (Retaliation)

P40. "Because she was jealous of my position within the company and wanted to make me look bad." (Envy)

Third, the *malevolent personality* of saboteurs also instigated their knowledge sabotage actions. In the eyes of targets, saboteurs were generally malevolent individuals (i.e. spiteful, lazy, selfish and egoistic people who were always trying to hurt someone) who had a very poor attitude toward others, who liked to play jokes on other – especially new – employees and who had various psychological issues contributing to their negative behavior:

P50. "She is selfish and inconsiderate. She doesn't care what happens to others." (Malevolence)

P102. "My co worker [. . .] didn't care enough about making an effort to do it right for me." (Poor Attitude)

P22. "I am told by other co-workers that she does this to all the new people. I guess I just asked the wrong person for help." (Joke's Target)

P5. "He was having some personal problems going on and was not thinking straight." (Psychological Issues)

In a vast majority of cases, saboteurs acted consciously and intentionally against their targets:

P28. "A colleague who was not fond of me tried to find ways to get me in trouble a lot."

Several cases were driven by the saboteurs' intentions to save the financial resources of their organizations while disregarding the ethical norms and causing direct harm to others. For example,

P6. "I think the company encouraged her [the manager] to give out as few bonuses as possible." (Money-Saving)

4.5 Impact

Table IV summarizes three types of impact of knowledge sabotage – on the target, the organization and the third party.

4.5.1 Impact on the person. The primary goal of saboteurs was to create a negative impact on their targets and they were able to achieve this in the vast majority of incidents. As a result, targets dramatically reduced their *work efficiency* because they had to engage in useless activities, waste time, duplicate knowledge possessed by other organizational members, educate themselves, re-do the tasks that were previously done incorrectly, miss or be late for work and re-schedule missed engagements. For example,

P58. "It made all the work I had done worthless and I had to start over."

P93. "It caused me to be late for an important project meeting with my supervisor."

Many incidents had a *psychological impact* on the targets when they were publicly humiliated in front of their managers and colleagues and put under pressure, which resulted in stress and various negative emotions. The highly expressive quotes below speak for themselves:

P26. "[. . .] it made me look like a complete idiot in front of our CEO and senior directors."

P69. "[. . .] it caused embarrassment and it upset me emotionally."

P93. "The mistake of not using the most current procedure really made me look incompetent."

Table IV Impact

Provoked type	*Unprovoked type*
On the person Impact: 81%; no impact: 19% Impact type: – Lower job efficiency – 36% – Time loss – 30% – Missing work/being late – 6% – Psychological impact – 20% – Public humiliation – 18% – Stress and pressure – 2% – Career impact – 19% – Official reprimand – 11% – Impeded career – 4% – Voluntary resignation – 2% – Wrongful dismissal – 2% – Direct financial impact – 6%	On the person Impact: 78%; no impact: 22% Impact type: – Lower job efficiency – 39% – Time loss – 33% – Missing work/being late – 6% – Career impact – 21% – Official reprimand – 13% – Wrongful dismissal – 4% – Impeded career – 3% – Voluntary resignation – 1% – Psychological impact – 14% – Public humiliation – 11% – Stress and pressure – 3% – Direct financial impact – 4%
On the organization Impact: 67%; and no impact: 33% Impact type – Failed/delayed project – 30% – Time loss – 19% – Direct financial impact – 6% – Being out of stock – 5% – Loss of client – 3% – Being understaffed – 2% – Lower quality – 2%	On the organization Impact: 63%; and no impact: 37% Impact type – Time loss – 29% – Failed/delayed project – 20% – Lower quality – 5% – Loss of client – 4% – Being understaffed – 3% – Direct financial impact – 2%
On the third party – Negative impact – 13%	On the third party – Negative impact – 5%

> P85. "I spent the next several months feeling pressured, insecure and uncomfortable."

In addition to experiencing a negative affective state as a result of a knowledge sabotage incident, many targets indicated that the event *jeopardized their career* because they were formally reprimanded or denied promotion:

> P104. "There was an external audit, and I was reprimanded of not doing my job diligently enough."

> P20. "I wasn't [the] lead marketer for a two month period."

> P43. "This also rendered me unable to perform certain types of sales I had just been trained to do."

> P2. "I [. . .] lost a chance at a promotion."

In several extreme situations, innocent individuals were *wrongfully dismissed* (i.e. fired) or decided to *voluntarily quit* their organization because they did not want to work in a place where similar events take place. For instance,

> P11. "I was terminated for doing it the next day."

> P67. "I realized that the owner had been looking for ways to get rid of me since before the birth and this was the final straw [. . .] I didn't want to continue working there at a lower pay and status."

> P51. "I took the blame [for] having prepared the log incorrectly and for missing the deadline. This affected my relationship with the partners in the firm and ultimately contributed to my eventual departure from the firm."

Some incidents produced a *direct negative financial impact* on the targets who were demoted, received a lower pay or had to pay a fine:

> P44. "I lost 2 hours worth of paid time that day."

> P43. "I got paid less and was unable to work the additional hours."

> P87. "I was fined 50$ by management on my first night!"

4.5.2 Impact on the organization. Even though saboteurs very rarely acted against their organizations, approximately two-thirds of all incidents resulted in various unanticipated organizational-level consequences. The first major category pertained to *time loss* when employees simply wasted their paid time, worked extremely inefficiently and had to re-do their work multiple times. In most incidents when employees wasted their paid time, their organizations had to pick up the bill. Consider, for example, the incident below:

> P7. "One of the other employees at my job came up to me and told me I was doing a procedure wrong. I was pretty sure I was correct, but I redid them like she told me to. Then I was told by the supervisor that I was doing it the wrong way, and had to fix everything again [. . .] I had to redo it twice [. . .] They [. . .] did not like me."

Here, the saboteur clearly acted against a fellow co-worker because of a personal dislike. An unanticipated consequence of her action was a certain amount of paid time wasted by the target who had to do the same task three times (i.e. first time correctly, second time incorrectly and third time correctly). In other words, their organization paid triple the rate for this amount of work.

Failed and delayed projects, which constituted 30 and 20 per cent of the provoked and unprovoked categories of knowledge sabotage, respectively, also emerged as a major unanticipated organizational impact. Such incidents had a more detrimental impact than employee time loss because it affected multiple workers or even entire departments. Consider, for instance, the incident below where the entire information system had to be redesigned, which involved additional man-hours, training expenses and reduced efficiency due to the organization's inability to use the needed technology by the deadline – only because the head of the client relations department deliberately provided incorrect data:

> P47. "I was in charge of quality control in our organization. We had a new technology being introduced and I was heading the project to make sure it did not have a negative impact on quality. In order to do this, I needed timely data from the developers on what to expect. The person in charge of the client relations in the development section of our company intentionally gave me incorrect data. He did this so that I would not have time to reject his work altogether and make him start over. He was basically putting his work load, and desires, ahead of call quality and since he knew I would go above his head to stop it, he lied to me to keep me in the dark [. . .] The new application was a failure from a quality standpoint and had to be redesigned [. . .] This made me have to devote more man hours to retraining the agents on the new application."

The organizational consequences of other cases where projects were delayed were definitely more far-reaching than saboteurs initially envisioned. For instance, a delayed quote sent to a customer may result in a missed sale, waiting for new equipment may slow down the production line and working late or doing overtime not only requires additional financial resources but also puts unnecessary pressure on employees and lowers their morale:

> P35. "It caused me to delay the quote to our clients."

> P86. "It delayed the purchase of new equipment for everyone."

P106. "It set my team and I behind a lot and [I] had to work overtime to fix it. Stay late night while the shop was closed."

In addition to the two major consequences discussed above, several smaller yet extremely important categories emerged. First, the incident had a *direct financial effect* on organizations, which, again, was not the saboteurs' intentions:

P32. "I also wasted materials for the first half dozen attempts, until I understood what was wrong with the instruction I had been given."

P54. "[. . .] the company lost profit due to giving the client the discount for the wrong order."

P85. "The dog [incident] caused thousands of dollars worth of damage and vet bills."

Second, *lower quality of output*, including products and services, was also reported by a number of knowledge sabotage targets. For example,

P72. "[We had a] subpar collection of investment choices."

P89. "The project room was not set up correctly and several protocols had not yet been put in place."

Third, the *loss of a client*, which, in turn, reduced the overall profit, was also reported by a number of knowledge sabotage targets:

P92. "I was unable to sign up the client [. . .] [because] I lost time on other projects while clearing up the problem."

P94. "Lost a few jobs because they [the customers] didn't want to deal with the company."

Fourth, due to knowledge sabotage incidents, in rare yet important cases, organizations ended up being *understaffed* or *out of stock*. For example,

P25. "We were short on our orders for the week and had to order garments from the regional stockroom, which took an additional 3 days."

4.5.3 Impact on the third party. The third-party was extremely rarely intentionally targeted by knowledge saboteurs. Nevertheless, the third party suffered in 13 and 5 per cent of all provoked and unprovoked knowledge sabotage incidents, respectively. A majority of cases pertained to clients who were inconvenienced and/or suffered financially. For instance,

P4. "It had a huge impact because I had to annoy the client that moved and the client had to re-transport the goods themselves because there wasn't any way for me to reroute it."

P8. "I had to re-deliver a section of the class because of the advice he gave me."

Moreover, in the extreme excerpts presented below, the unanticipated damage caused by saboteurs led to both emotional and physical suffering:

P65. "I was in need of a referral which would allow the client to remain in the home with supports. I needed the supervisor to sign off on this because she was licensed at a higher level than myself at the time. [Instead,] she submitted a recommendation of a skilled nursing facility [. . .] This resulted in turmoil for a client and his family. [T]his is the aspect of the situation I find most disturbing. The client was forced to remain in a more restrictive environment as I worked to meet the protocols necessary to discharge the client home."

P95. "Being a nurse the end of shift report where the off-going nurse gives report to the oncoming nurse is extremely important. A few months ago a fellow nurse failed to report the findings of a newly developing bedsore. The bedsore increased in size and depth during my shift when an intervention could have been started."

4.6 Attribution of responsibility

As expected, the saboteur was the leading culprit who caused the incident (Table V). Surprisingly, 19 and 13 per cent of the targets of provoked and unprovoked knowledge sabotage events, respectively, blamed both the saboteurs and themselves. Another interesting finding is that nobody blamed a single party for the incident (except for the saboteur) and the responsibility was assigned to both the saboteur and the organization, the saboteur and the manager or the organization and the manager. In such cases, the targets blamed not only the saboteur but also their organization and the manager who let this incident happen.

4.7 Attitude and behavior change toward the saboteur

Table VI summarizes targets' changes in their attitude and behavior toward saboteurs.

A vast majority of targets changed their attitude and/or behavior toward saboteurs. The major type of changes in attitude pertained to a *lack of trust* in the future knowledge provided by the saboteur responsible for the incident. As a result, targets no longer trusted anything saboteurs did or said, became suspicious of their assistance and started watching themselves when interacting with these individuals:

> P10. "I learned not to trust her with any type of information that she gave me."

> P20. "I no longer trusted him after that, and still do not to this day."

After an incident, many targets started to verify all information provided by the saboteur:

> P28. "I still acted professionally but would confirm orders with my boss from there after."

> P89. "[. . .] if they gave me information, I would triple check it with other sources. Additionally, I learned to confirm all client site visits directly with the client."

Table V Attribution of responsibility

Provoked type	*Unprovoked type*
The saboteur – 66%	The saboteur – 70%
The saboteur and myself – 19%	The saboteur and myself – 13%
The saboteur and the organization – 10%	The saboteur and the organization – 9%
The saboteur and the manager – 4%	The saboteur and the manager – 6%
Myself – 1%	The organization and the manager – 2%

Table VI Attitude and behavior change toward saboteurs

Provoked type	*Unprovoked type*
Yes – 86%; no – 14%	Yes – 77%; no – 23%
Type of changes:	Type of changes:
– Changes in attitude – 48%	– Changes in attitude – 51%
– Lack of trust – 36%	– Lack of trust – 40%
– Negativity – 12%	– Negativity – 11%
– Changes in behavior – 38%	– Changes in behavior – 26%
– Avoidance – 29%	– Avoidance – 16%
– Lack of knowledge sharing – 5%	– Lack of knowledge sharing – 5%
– Hostility – 4%	– Hostility – 3%
	– Other – 2%

One individual went as far as documenting all subsequent interactions with the saboteur:

> P69. "I also documented my interactions with her so things like this would not happen again and if they did I would have a way of protecting myself. I made sure other people were present during our interactions."

In some situations, the targets extended their distrusting attitude onto the other organizational members. For instance,

> P26. "I lost faith in some of my co-workers and relied only on myself. I learned to watch my back, not matter how kind someone may seem at first. I also learned to do my own research and never do something just because someone told me to do something."

> P92. "I now verify any information I am given."

On the one hand, the targets' behavior is reasonable because they need to protect themselves from similar incidents in the future. On the other hand, this causes two major issues. First, it creates an environment of suspicion, especially when others observe and copy such distrustful behavior. Second, a need to verify and double-check information with others creates inefficiencies, loss of time and unnecessary distraction – all of which reduces productivity.

The second category of attitudinal change pertained to *strong negative feelings* toward saboteurs such as disgust, dislike, hate and disrespect:

> P11. "I despise that person for wrecking my career."

> P81. "I lost a lot of respect for my superior, and I started viewing him as very immature and childish."

In addition to attitudinal changes, around one-third of the targets also altered their behavior toward saboteurs. The major behavioral change pertained to *avoidance* when targets limited their interaction with saboteurs and avoided them in a professional setting. For instance,

> P3. "I realized this person was someone to be avoided at all times. She was unprofessional, and not just damaging to me, but she gave no thought to the consequences for our clients who would have received bad information."

> P27. "[I] never spoke to this one again and went over her head."

Many went as far as formally refusing to work with the saboteur in the future:

> P74. "I did not want to work with a liar so I asked the manager I would like to move to another store."

> P97. "I refused to work with the[m] or cooperate with them ever again."

Most importantly, those who experienced a knowledge sabotage incident became suspicions of these saboteurs, stopped trusting their knowledge and never approached them for help in the future, which undermined the very principles of intra-organizational knowledge sharing:

> P15. "I really watched myself around this person and refused to go to them anymore for information."

> P16. "I always watched my back and did not ask him for any help on anything."

In addition, the avoidance behavior was occasionally transferred onto the non-work relationships between targets and saboteurs, thereby terminating friendships and personal communication:

P32. "We used to ride to work together (I picked him up and he rode with me) and had what I thought was a good rapport. I considered him to be a friend. Afterwards, I cut off all contact with him."

P51. "[. . .] on a personal level, I rarely communicated with her or acknowledged her after that incident. Previously, we had maintained a cordial relationship."

Some targets also *stopped sharing their knowledge* with the saboteurs. For example,

P89. "I no longer volunteered information to help this person."

P57. "I no longer helped the person out when they needed it."

A few started to openly express *negative and hostile emotions* and behaviors toward the saboteurs and considered them an enemy:

P6. "I got angry and hostile."

P68. "I was no longer friendly with this individual."

Those who did not change their attitude and behavior toward saboteurs were classified into two distinct groups. In the first, larger group, people did not change their attitude because they decided to behave in a professional manner and did not let their personal feelings affect working relationships. For instance,

P37. "I was angry, but business is business. I try not to let personal feelings intervene."

P34. "No, I continue to be professional."

In the second, smaller groups, targets had already known that the saboteur had a shady reputation and were not surprised with their unethical behavior. Thus, they had developed a negative attitude toward this individual before the knowledge sabotage incident took place and they did not change it afterward,

P31. "No, I already didn't really like him very much."

P8. "No because I wasn't really all that fond of this person to begin with."

4.8 Attitude and behavior change toward the organization

Table VII presents the targets' changes in attitude and behavior toward their organizations.

The results indicate that the majority of the targets did not change their attitude or behavior toward their organization because most of them attributed the incident solely to the saboteur. As some of them indicated,

P101. "The origination had nothing to do with the event. It was solely based on one person."

Table VII Attitude and behavior change toward organizations

Provoked type	*Unprovoked type*
Yes – 24%; no – 76%	Yes – 29%; no – 71%
Type of change:	Type of change:
– Changes in attitude – 23%	– Changes in attitude – 27%
– Negativity – 19%	– Negativity – 25%
– Lack of trust – 4%	– Lack of trust – 2%
– Changes in behavior – 1%	– Changes in behavior – 2%
– Reduced work effort – 1%	– Reduced work effort – 2%

P80. "Full blame goes to the worker."

At the same time, even though only about a quarter of the respondents altered their attitude or behavior toward their organizations, the change was extremely negative, drastic and long-lasting. For example, in terms of attitude change, those who developed a feeling of *negativity* toward their organization indicated the following:

P85. "[. . .] it has always made me have bad feelings about the company."

P49. "I detest them [. . .] I want nothing ever again to do with them. I worked so hard for them - even went in on the weekends. And I got less than nothing in return."

Those who reported a *lack of trust* in their employer stated that they became more diligent and distrustful toward other organizational members to avoid becoming a victim of knowledge sabotage in the future. For instance,

P97. "I am now much more weary of any proposals given to me by other researchers at our University, and I am much more cautious about accepting and analyzing samples that I did not prepare myself."

P75. "I made sure I double checked everything in the future."

In addition, a few targets reported decreased work effort due to their frustration with the organization. For example,

P6. "I stopped trying to be a good employee because I felt like there was no point."

4.9 Retaliation

Only two and three percent of the targets of provoked and unprovoked knowledge sabotage incidents, respectively, indicated that they engaged in retaliatory behavior against saboteurs by means of knowledge sabotage. For instance, an employee who received incorrect knowledge on the preparation of a report from a colleague because of a personal conflict tried to get even later:

P62. "Yes, I told her incorrect information about a new procedure later on."

Those who decided not to retaliate did so for moral and ethical reasons or because they were afraid of the repercussions of their action. For example,

P108. "No, I have better work ethic than that."

P30. "I never tried this because I knew how much problems that can bring."

4.10 Incident reporting

In total, 48 and 29 per cent of the targets of provoked and unprovoked knowledge sabotage incidents, respectively, formally or informally reported the infraction (Table VIII).

A majority complained to their managers or other superiors, some informed other employees and a few sought assistance of the human resources office or the union. For example, the respondents indicated the following:

P76. "I sent out a message to the department [manager] informing them that I was given bad information and would have to re-do the schedule."

P21. "I told a couple of my close coworkers and they were more aware of what [a person's name is removed for anonymity] was like."

Table VIII Incident reporting

Provoked type	*Unprovoked type*
Yes – 49%; no – 51% Complained to: – The manager/superior – 38% – Other employees – 6% – The human resources office – 3% – The union – 2%	Yes – 29%; no – 71% Complained to: The manager/superior – 28% The human resources office – 1%

Those who chose not to report the infraction did so for three primary reasons. First, the targets believed that doing so was useless because management would not do anything against the saboteurs. For instance,

> P10. "I knew it would have fallen on deaf ears since others had already complained [. . .] because any type of complaint against her never ended up anywhere."

Second, the targets believed that they could not corroborate their story to prove the saboteurs' wrongdoing. For example,

> P80. "I did not have 100% proof and making an allegation of this nature would have been really bad."

Third, the targets simply did not want to deal with the situation any further and experience additional stress, but some of them considered the possibility of informing others about the incident in the future. For example,

> P26. "I decided to mind my own business but will definitely be speaking to my supervisors when I leave the organization."

At the same time, a few respondents who did not report the incident later regretted their decision:

> P65. "I unfortunately did not report this situation, but I should have. I should have reported it because her future actions could have made major impacts on the quality of clients lives."

Table IX summarizes the actions taken against saboteurs resulting from targets' complaints.

Regrettably, in over one-third of all cases, no action was taken. In almost one-third of all cases, the targets were not informed about the outcome of their complaint. In many cases, complaints were dismissed, targets were blamed and no action against saboteurs was taken. For instance,

> P6. "I told my supervisor about it, and she just said 'well you should do it like it says in the manual'."

Table IX Action against saboteurs

Provoked type	*Unprovoked type*
None – 36% Fired – 19% Reprimanded – 10% Transferred – 2% Other – 2% Unaware of the consequences – 31%	None – 50% Transferred – 11% Other – 11% Unaware of the consequences – 28%

P85. "Yes[, I complained to] the store manager but nothing changed. She tortured me until I found another job."

In such situations, some respondents were so disappointed with their organizations or colleagues that they decided to quit their job or move to another department. For instance,

P7. "I left when it became clear that I could not have my side of the story heard. I didn't value a job where I was treated as such."

P16. "The department supervisor wondered why the report was taking longer than he expected. I said I had used the wrong information that was given to me, but I was contradicted by my immediate supervisor. He was believed [. . .] I transferred to a different department the next year."

However, in situations when management acted, the consequences were generally extremely severe because most saboteurs were terminated, transferred to the other parts of their organizations and formally reprimanded:

P90. "The information was reported to my supervisor. [T]he employee was not in the building when I returned and never appeared again, even refusing to pick up her final paycheck to avoid being confronted."

P52. "I reported it to my manager after I had found out it was really taking place. They were assigned to a different team shortly after that."

P107. "I reported the incident to my supervisor. She filed an incident report to put in [a person's name is removed for anonymity] employee file."

4.11 Other findings

During the analysis, several additional findings emerged. *First*, even though the word "sabotage" was never mentioned in the study's description, situations and questions, many respondents mentioned it in their responses. As such, they believed that their colleagues or managers purposely engaged in sabotaging behavior by deliberately supplying them with incorrect knowledge. The quotes below further confirm the validity of the knowledge sabotage concept:

P45. "My coworker tried to sabotage me by giving me faulty information about a client."

P66. "I feel like he wanted to sabotage me."

P51. "I think she felt threatened that I would be given some larger role in working on this high profile case, so she wanted to sabotage me."

P59. "[. . .] my ex boss had the habit of sabotaging other's work [. . .]"

Second, almost one-third of all knowledge sabotage incidents were driven by personal career and gain motivations of saboteurs. In such situations, saboteurs engaged in highly unethical behavior to get ahead of their fellow employees when competing for a promotion, a raise or another tangible reward. Consider, for example, the following incident:

P70. "This happened 5 years ago when I started out as a temp at the company. There was another female temp there working along side me. We were told that only one of us would get a permanent position at the end of the season. There was an instance when I asked her for some information about the client due date and I know she deliberately gave me false information [. . .] because she was to see me fail and get the full time position for herself."

As such, both employees were put into an extremely difficult situation because they had to choose missing a permanent position or securing it by any means. Thus, their organization

and management were equally responsible for the knowledge sabotage incident above. In other similar incidents, it was the actions of management that fostered an extremely unhealthy, competitive culture where employees had to take advantage of one another by any means. For instance, several respondents indicated the following:

> P89. "[. . .] the company was well aware that many of the middle managers were very cut throat and they encouraged the behavior in a sense. The toxic culture eventually made me realize I needed to look for a different company to work for."

> P56. "I was working at a company that did stack-ranking and competition was brutal and vicious [. . .]"

> P77. "When I just started my first job I felt that there was a fierce competition among employees in the department [. . .]"

Third, overall, very few differences between the provoked and unprovoked types of knowledge sabotage were observed. At the same time, during unprovoked knowledge sabotage incidents, saboteurs were more likely to supply intangible knowledge. Targets of unprovoked knowledge sabotage incidents were less likely to report the incident: only 29 per cent of them did so compared to 48 per cent of the provoked knowledge sabotage targets.

Fourth, the process of active knowledge sabotage discussed above may be represented as a visual diagram (Figure 3). It depicts the driving force, the type of transmitted knowledge, the intended target, the negative impact, the victims' attribution of responsibility and their subsequent changes in attitude and behavior, incident reporting and actions taken against the saboteurs after a formal complaint.

5. Discussion

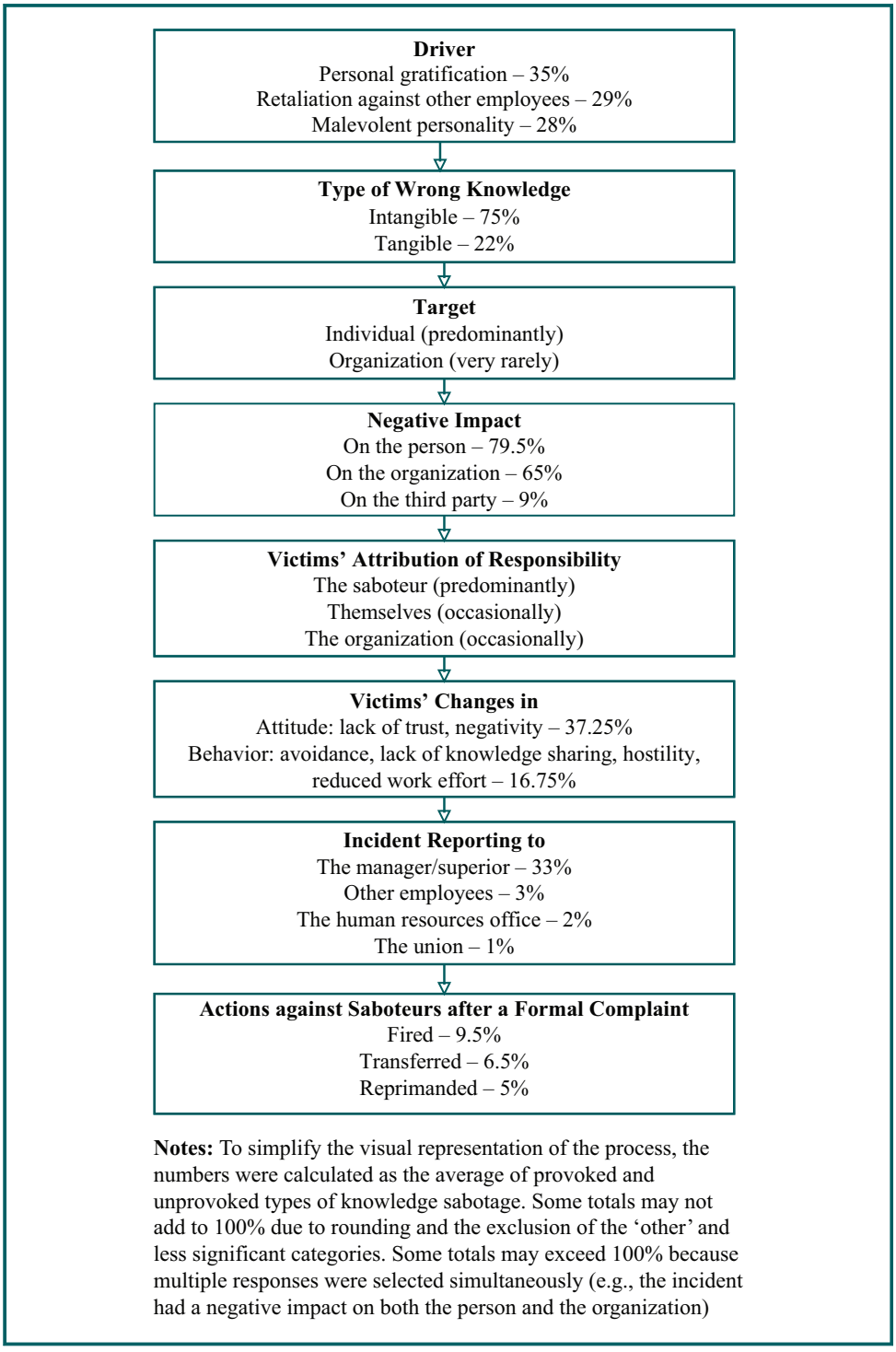
In total, 109 knowledge sabotage targets who reported 172 critical incidents offered a unique perspective explicating the phenomenon, which extends the results of the previous study by Serenko (2019), who focused on knowledge saboteurs. Based on the findings, a number of theoretical and practical implications emerged, warranting further elaboration.

5.1 The integration of the saboteurs' and targets' perspectives

The present investigation dramatically extends the findings reported in the previous study of knowledge saboteurs. Table X integrates both perspectives and shows that both knowledge saboteurs and their targets believe in their innocence – saboteurs are certain that their action was a necessary response to targets' inappropriate workplace behavior, whereas targets insist on their innocence and hold saboteurs solely responsible. In cases of interpersonal conflict, dramatic discrepancies were observed between how saboteurs [as documented by Serenko (2019)] and targets view themselves. Both parties believe that they are completely innocent: saboteurs view themselves as victims of the targets' poor behavior and performance who, unwillingly, had to retaliate, whereas targets consider themselves knowledge sabotage victims who never deserved such treatment. From the perspective of saboteurs, they (the saboteurs) intentionally engaged in knowledge sabotage to punish someone who exhibited a negative, hostile and disruptive behavior; caused a great degree of harm; never put enough effort into their job; took advantage of others; never helped anyone; and was incompetent. From the viewpoint of targets, saboteurs are spiteful, selfish, egoistic, lazy, envious and conflict-prone individuals who generally dislike others and even exhibit mental problems. In other words, both parties attribute the cause of an incident to each other while insisting on their innocence.

The phenomenon above may be explained from the perspectives of conflict asymmetry (Jehn *et al.*, 2010) and attribution theory (Kelly, 1972; Weiner *et al.*, 1972). Conflict

Figure 3 The process of active knowledge sabotage



Notes: To simplify the visual representation of the process, the numbers were calculated as the average of provoked and unprovoked types of knowledge sabotage. Some totals may not add to 100% due to rounding and the exclusion of the 'other' and less significant categories. Some totals may exceed 100% because multiple responses were selected simultaneously (e.g., the incident had a negative impact on both the person and the organization)

asymmetry suggests that people differ in their perceptions of the amount of conflict they experience in a dyadic relationship. For example, when two individuals have a conflict, one may consider it an extremely important event, whereas another may totally dismiss it. Thus, it is possible that targets remained virtually unaware of the existence of a conflict while saboteurs considered it an extremely critical event requiring further action. Attribution theory

Table X Mental presentation of saboteurs vs targets – the integration of both perspectives

	Saboteurs	*Targets*
View themselves	Completely innocent Victims of the targets' poor behavior and performance	Completely innocent Victims of knowledge sabotage
View their opponents	Exhibit negative, hostile and disruptive behavior Cause harm to others Lazy and unproductive Incompetent Unhelpful	Spiteful, selfish and egoistic Lazy Extremely envious Dislike others Are conflict-prone Have mental issues
Motivation	To punish those who deserve it	To punish the innocent

posits that people attribute positive events to themselves (e.g. "I succeeded because I worked hard") and negative occurrences to others (e.g. "I failed because of someone's unexpected action"). It is likely that targets attributed the cause of the saboteurs' actions solely to saboteurs themselves and completely dismissed the fact that they might have somehow instigated their behavior.

5.2 Contribution to theory

First, it was found that knowledge sabotage is a widespread organizational phenomenon. The pre-screening survey revealed that 54 per cent of employees had experienced at least one critical episode of knowledge sabotage and most of them had become knowledge sabotage victims multiple times. In over one-third of organizations, knowledge sabotage incidents take place at least occasionally and they have become regular events in around 7 per cent of organizations. In many cases, victims realize that the perpetrators intentionally committed an act of sabotage with a malicious purpose in mind.

The management literature is replete with examples of counterproductive workplace behavior such as social undermining (Duffy *et al.*, 2002), rudeness (Johnson and Indvik, 2001), emotional abuse (Keashly and Harvey, 2005), incivility (Blau and Andersson, 2005), bullying (Vartia, 2001), discrimination, aggression, harassment and violence (LeBlanc and Barling, 2005; Neuman and Baron, 2005; Krieger *et al.*, 2006). The present investigation empirically confirms that knowledge sabotage should become an unfortunate addition to the list above because it is a widespread organizational phenomenon. At the same time, it points to the similarities and differences between knowledge sabotage and the other types of counterproductive workplace behavior mentioned above. In terms of similarities, all of them go against the legitimate interests of an organization and its stakeholders, deviate from the conventional norms of appropriate behavior, violate multiple internal policies, break ethical principles and threaten the very existence of the entire organization. These behaviors disrupt organizational routines, lower production, reduce output quality and increase the voluntary turnover rate because some targets decide to quit their jobs to avoid future victimization. The perpetrators' actions are frequently driven by their egoistic desire for gratification, retaliation and malicious personality traits. Victims of counterproductive workplace behavior experience negative emotions, anxiety, stress and humiliation.

There are, however, two major differences between the previously documented types of counterproductive workplace behavior and knowledge sabotage. Many counterproductive workplace behaviors, for instance, workplace aggression, may be classified as organizational (directed against one's organization) or interpersonal (directly against a particular individual in one's organization) (Hershcovis *et al.*, 2007). While knowledge sabotage also fits this classification scheme, it was observed that a vast majority of knowledge sabotage incidents fall under the interpersonal category. This finding was somewhat unexpected because, in general, employees tend to sabotage their organization

more frequently than their fellow co-workers (Analoui, 1995). In addition, the other types of counterproductive workplace behavior often occur when employees believe that their organization has breached the psychological contract (Chao *et al.*, 2011), which informally delineates the mutual beliefs, perceptions and obligation between employees and their organizations (Rousseau, 1989; Robinson *et al.*, 1994). As such, employees' actions represent a response to the breach of the psychological contract. In contrast, knowledge sabotage is generally a response to interpersonal workplace problems. After the incident, victims may believe that their employer violated the psychological contract by allowing it to happen and failing to prosecute the perpetrator. Subsequently, victims may respond by adjusting their attitude and behavior or even leave their organization. Thus, the breach of the psychological contract is a consequence rather than a cause of knowledge sabotage.

The present study also demonstrates the existence of both provoked (when the target requested knowledge from the saboteur) and unprovoked (when the target did not request knowledge from the saboteur) types of knowledge sabotage and shows that the former type occurs approximately twice as often as the latter. Even though the unprovoked type of knowledge sabotage takes place less often, its very presence in the contemporary workplace is an alarming fact in itself. In such cases, the perpetrator may have extremely malevolent goals in mind when deliberately approaching an unsuspecting co-worker and providing him or her with wrong knowledge yet clearly realizing the harm it might cause to this person. As such, this behavior is not only counterproductive but also somewhat illegal.

Second, it was discovered that knowledge saboteurs are more likely to provide intangible than tangible knowledge. In over two-thirds of all incidents, knowledge saboteurs provided targets with intangible knowledge such as oral recommendations, advice or tips. This finding may be explained theoretically. The transmission of intangible knowledge is more difficult to corroborate than that of tangible knowledge existing in the form of reports, documents, templates, etc., which can be used as evidence against the perpetrator. According to deterrence theory, the likelihood of punishment is directly proportional to the probability of illicit action (Geerken and Gove, 1975; Pratt *et al.*, 2006). When knowledge sabotage victims launch a formal complaint against perpetrators, they can use tangible knowledge as evidence to prove their innocence. Thus, creating a formal paper trail may deter potential knowledge saboteurs. The communication of intangible knowledge also requires less effort and may be done impulsively at a mere opportunity to do so. Because people tend to minimize their cognitive effort (Fiske and Taylor, 1984; West, 2008) and their behavior is often driven by subconscious implicit cognition rather than by a rational assessment of the pros and cons of their action (Joseph, 1992; Greenwald *et al.*, 2009; Serenko and Turel, 2019), saboteurs may impulsively engage in a questionable behavior by verbally communicating wrong knowledge when an opportunity presents itself.

Third, it was concluded that knowledge sabotage is driven by three factors:

1. Gratification.
2. Retaliation against other employees.
3. One's malevolent personality.

Gratification drivers pertain to promotions, easier workload, monetary incentives and other extrinsic rewards. In such incidents, perpetrators use wrong knowledge to sabotage targets' performance, make them appear incompetent and force them to quit or get wrongfully dismissed. In other words, saboteurs engage in this counterproductive workplace behavior to secure personal benefits at the expense of their fellow co-workers and their entire organization. Such behavior often represents adverse reactions to perceived distributive and procedural injustice (Skarlicki and Folger, 1997). Distributive

justice is the perceived fairness of the distribution of compensation and rewards including money and promotions and procedural justice is the perceived fairness of the means used to determine this distribution (Folger and Konovsky, 1989). Saboteurs who are driven by gratification factors often believe that they are unfairly denied something of value and this perception likely results from an unjust incentive distribution or a biased distribution procedure. Consequently, they take matters into their own hands to restore justice while being totally inconsiderate of the suffering that their action may cause to their fellow co-workers.

Knowledge sabotage is also driven by *retaliation* against other employees. Conflict is an inevitable part of human relations and it is commonly present in all organizations. When employees have a conflict with their managers, colleagues or subordinates, they can feel that the quality of their interaction with others has been compromised. This phenomenon may be analyzed from the perspective of interactional justice, defined as the perceived quality (i.e. dignity, fairness, politeness and respect) of interpersonal treatment received from other organizational members (Bies, 2015). When employees believe that the norms of interaction have been broken, they may engage in organizational retaliatory behavior (Skarlicki and Folger, 1997), which has become so common that it is often regarded as being "part of the social fabric of the workplace" (Tripp and Bies, 2009, p. 1). Thus, knowledge sabotage serves as a mechanism for workplace revenge driven by interpersonal conflict and the perception of interactional injustice. In a similar vein, Semerci (2019) observed that inter-employee relationship conflict triggers counterproductive knowledge behavior.

The *malevolent personality* of saboteurs also serves as a major trigger of their knowledge sabotage behavior. Some individuals exhibit general cruelty or negative attitude toward others and a tendency to play jokes on the weak. In this case, knowledge sabotage is merely a tool for those who want to satisfy their ego or to entertain themselves.

Fourth, knowledge sabotage results in extremely negative consequences for individuals, organizations and even third parties. Knowledge saboteurs almost always act against other individuals rather than against their organizations but both the individual and organizational consequences of their behavior are more far-reaching than saboteurs originally intended. In a vast majority of incidents, saboteurs achieve their malicious goal – their targets are late for important engagements, publicly humiliated, stressed, reprimanded and denied promotions. Some of them even quit their jobs or are wrongfully dismissed. Saboteurs also gain some tangible benefits and satisfy their ego. At the same time, their organizations have to bear the burden of their behavior. In two-thirds of knowledge sabotage incidents, organizations experience a direct or indirect financial impact due to time waste, inefficiencies, delayed or terminated projects, lower output quality, lost clients and being understaffed or out-of-stock. Replacing a wrongfully dismissed worker is expensive and unwarranted terminations may result in legal action and damaging publicity. Moreover, resulting negative reviews of organizations, their managers and inter-employee relationships posted on social media websites (e.g. Glassdoor) may deter prospective job applicants and cause brand damage. In some cases, the damages even spread onto the third party including customers. As such, the overall organizational and third party losses dramatically exceed the personal benefits enjoyed by knowledge saboteurs.

In addition, after the incident, around a quarter of knowledge sabotage targets develop an extremely negative attitude toward their organization. This may result in various counterproductive behaviors including voluntary turnover and reduced effort, which, again, takes a toll on the overall organizational effectiveness and efficiency.

Fifth, even a single knowledge sabotage incident may dramatically impede intra-organizational knowledge flows. After an incident, most victims change their attitude and behavior toward saboteurs and even toward other employees, which develops an

atmosphere of mistrust, negativity, avoidance and hostility. Virtually all victims blame saboteurs for the incident. Some of them attribute the responsibility to saboteurs, as well as to their managers, their organizations and even themselves. Most likely, they believe that their managers and organizations are responsible for the prevention of this behavior and that they should have also avoided interacting with a potentially unreliable source of knowledge. Consequently, they do not wish to experience a similar incident and the most logical form of prevention is not to deal with the offenders and other employees who may engage in similar behavior. This impedes intra-organizational knowledge flow because knowledge sabotage victims do not engage in open communication, avoid their colleagues, distrust their knowledge and hide knowledge from others. While knowledge sabotage may be an isolated, one-time event, its repercussions may haunt victims for their entire tenure with their organizations.

Sixth, most knowledge sabotage victims do not retaliate against perpetrators by means of knowledge sabotage; instead, they develop cognitive responses and coping strategies. Previous research suggests that, when employees are treated unfairly by their colleagues or administration, they engage in various forms of retaliatory behavior (Skarlicki and Folger, 1997; Tripp and Bies, 2009). Thus, it seems reasonable to assume that knowledge sabotage victims may retaliate against the perpetrators by using a similar and/or more sophisticated knowledge sabotage strategy (i.e. a "tit for tat" approach). In contrast to expectations, this proposition was empirically refuted because virtually all targets choose not to engage in retaliatory behavior for moral reasons or because of the fear of punishment. Instead of retaliation, they produce cognitive responses and coping strategies such as developing a negative attitude and distrust toward saboteurs, avoiding them and verifying everything they share with a trusted party. Some of them also develop a negative attitude toward their organization.

Seventh, in some situations, knowledge saboteurs may be held accountable for their actions. Less than half of all targets complain about the incident to their managers, the human resources office, the union or other employees. In the majority of complaints, either no action is taken or the results are never communicated to or noticed by the complainant. However, in rare cases when the action is taken, the outcome is very drastic for knowledge saboteurs who are fired, reprimanded or transferred to other units. On the one hand, most saboteurs are able to conduct their questionable actions with impunity. On the other hand, if the incident is properly investigated and acted upon, the punishment is very severe.

Eight, organizations often act as facilitators of knowledge sabotage among their employees. Even though knowledge sabotage acts are deliberately committed by individual employees, in many cases, organizations are partially responsible for the existence of this extremely unethical and unproductive behavior. Organizations often create a highly competitive culture driven by extrinsic motivation (e.g. a zero-sum game-based reward structure) and fear (e.g. the fear of losing a job when only one of two temporary employees will be granted a permanent position). When placed under extreme pressure when one's gain must be equally balanced by another's loss, even very conscientious workers may engage in questionable practices, including knowledge sabotage. In addition, organizations often lack policies to address and resolve knowledge sabotage complaints and to offer victim support. As a result, fewer targets raise their concern and the incidents remain unnoticed, which promotes subsequent knowledge sabotage behavior.

Ninth, knowledge sabotage may be introduced as an additional variable in the existing KM frameworks and models. For instance, the Socialization, Externalization, Combination, and Internalization (SECI) model is based on the principle of veracity (Nonaka and Konno, 1998), but the dynamics within the model and players' behavior may change by introducing the possibility of deliberately injecting incorrect knowledge or consciously withholding critical pieces of knowledge, which may lead to entirely different outcomes. If knowledge sabotage is present in the organization, wrong explicit knowledge may be deliberately

injected into organizational routines and it may be eventually internalized and transformed into a tacit form. At this point, it may be extremely difficult to identify and correct the issue. Moreover, the mere possibility of encountering wrong knowledge may change employee attitude and behavior by making them less willing to accept knowledge from others. In this case, the very underlying principles of the SECI model may be jeopardized. The injection of the wrong knowledge may also influence the relationship between organizational size and internal knowledge flows (Serenko *et al.*, 2007). Such propositions, however, warrant thorough empirical investigation in future research.

Tenth, social desirability bias is present in the description of knowledge sabotage incidents from the saboteurs' perspective, despite full anonymity conditions. While there are many similarities between the perspective of knowledge saboteurs documented earlier (Serenko, 2019) and that of knowledge sabotage targets observed in the present study, there are also several stark differences. With respect to similarities, *first*, both studies observed that a majority of saboteurs acted against their colleagues and managers. *Second*, very few saboteurs purposefully acted against their organizations. Both studies documented the extremely negative, unanticipated organizational consequences of knowledge sabotage such as a waste of time and resources, failed and delayed projects and lower output quality. Occasionally, the unanticipated harm spread onto the third party. *Third*, personal gain when saboteurs acted in their own interest was consistently identified as one of the very important motivational factors. *Fourth*, both studies observed a similar impact of knowledge sabotage on the targets who were humiliated, stressed, reprimanded, wrongfully dismissed, wasted work time, missed deadlines and quit their jobs.

In terms of differences, *first*, during a pre-screening phase in the previous study (Serenko, 2019), 42 per cent reported causing a knowledge sabotage incident at least once. At the same time, 54 per cent of those surveyed in the present study mentioned being a target at least once. *Second*, in the present study, targets indicated that some saboteurs were fired after a formal complaint. In contrast, in the previous study (Serenko, 2019), none of the saboteurs admitted to being fired for engaging in knowledge sabotage. This means that knowledge saboteurs accurately depict the event and its impact on others, but they tend to withhold negative information pertaining to the personal repercussions of their action, despite the condition of full anonymity. It is also possible that individuals who were previously fired for engaging in knowledge sabotage misrepresent events during a survey or avoid participating in sabotage studies because it may trigger negative memories. As such, social desirability bias is still present in the description of knowledge sabotage incidents from the saboteurs' perspective. At the same time, knowledge sabotage targets probably offer a less biased perspective as documented in the present study.

5.3 Contribution to practice

The theoretical insights above lead to several practical recommendations, which may be of interest to various knowledge managers and policymakers. *First*, it is recommended that organizations recruit employees with compatible personalities and working styles. Managers need to realize that all individuals have their own unique characters and work preferences, which are very difficult to control and modify. Interpersonal incompatibilities because of irreconcilable differences in employees' personalities and task conflicts arising from disagreement on how to perform work-related activities may result in strained relationships and possible retaliation by means of knowledge sabotage. Thus, organizations should strive toward the homogeneous workforce in terms of employees' personalities and working preferences (but not with respect to knowledge, experience, education, etc.) because doing so may substantially reduce (but not entirely eliminate) knowledge sabotage instances. However, recruiting the homogenous workforce may not be feasible, particularly in industries experiencing a tight labor market. *Second*, to prevent knowledge sabotage, organizations are recommended to introduce inter-employee conflict prevention and

resolution policies. Despite the best intentions to achieve the homogenous workforce, completely eliminating all instances of inter-employee conflict is unrealistic. The problem is that, when employees try to resolve the conflict by themselves and take matters into their own hands instead of focusing on a win-win, peaceful solution, they may engage in the "tit-for-tat" war-like games and use knowledge sabotage as a tool for revenge. Therefore, conflict management should become a key focus of organizational policies. Ideally, conflicts should be prevented and de-escalated by involving a team of conflict management professionals and individual employees should be discouraged from trying to resolve the situation on their own. For this, organizations are encouraged to develop and implement conflict prevention and resolution policies, which may suppress knowledge sabotage behavior and save tremendous organizational resources.

Third, organizations should develop clear and specific anti-knowledge sabotage policies. Most organizations have a variety of policies pertaining to technologies (e.g. e-mail usage rules), operations (e.g. manuals) and inter-employee relationships (e.g. anti-bullying). It is recommended that they extend this list by including knowledge sabotage as a form of counterproductive workplace behavior. As a starting point, organizations may consult general anti-sabotage policies already existing in some organizations and, especially, in the military, where sabotage has been used for centuries from a strategic perspective. *Fourth*, in addition to having anti-knowledge sabotage policies, managers should clearly articulate the individual and organizational consequences of knowledge sabotage. As such, the individual and organizational consequences of knowledge sabotage are truly devastating, ranging from minor incidents of wasting paid worktime to major debacles such as wrongful dismissals, lost clients, damaged brands and failed projects. Very few knowledge saboteurs predict a larger-scale individual and organizational impact of their presumably innocuous behavior, but their personal extrinsic and intrinsic gains may cost their co-workers and employers dearly. One possible knowledge sabotage prevention approach may focus on educating employees on the overall magnitude of such behavior and appeal to their sense of organizational citizenship. For example, they may be provided with hypothetical or real examples of knowledge sabotage and its unanticipated consequences for various stakeholders. While some employees may still disregard this information and pursue their egoistic motives, others may re-consider their engagement in knowledge sabotage.

Fifth, organizations are advised to completely eliminate zero-sum game-based incentives and rewards. It is not surprising that, when put under extreme pressure when one's gain is another's loss, employees disregard the well-being of their fellow colleagues and achieve their egoistic goal by any means, including knowledge sabotage. Thus, it is likely that by eliminating zero-sum game-based compensation, promotion and reward incentives, organizations may reduce the number of knowledge sabotage incidents by up to 30 per cent. For instance, temporary employees should not compete with others for a permanent position and the compensation of sales representatives should not be solely linked to their individual performance. The key purpose is to remove the incentives leading to the perception of competition among employees for a limited pool of rewards.

5.4 Limitations and future research directions

No scientific endeavor is perfect and the present investigation is no exception. *First of all*, because only respondents residing in the USA were allowed to take part in this study, the generalizability of the findings above should be tested in other countries. According to Henrich *et al.* (2010), most people are not western, educated, industrialized, rich and democratic – individuals living in the Western countries, including the USA, differ from their non-western counterparts in terms of their reasoning, values and behaviors. The models and theories created and tested in the western context may not always apply in the contexts of other countries (Palvia *et al.*, 2017). It is feasible that employees from non-western countries may engage in workplace sabotage for different reasons or respond to

knowledge sabotage incidents in a different manner. *Second*, through the integration of the saboteurs' and targets' perspectives, the present study identified irreconcilable differences between the parties. However, theory and practice would benefit from knowing the exact sources of the disparity between the views of knowledge saboteurs and their targets. *Third*, it was observed that knowledge saboteurs are more likely to use intangible than tangible knowledge. However, it is important to obtain solid empirical evidence to understand the reasoning affecting the saboteurs' preferences, which may lead to important theoretical and practical implications.

Fourth, the finding that the malevolent personality of saboteurs is a major driver of their malicious behavior represents a fruitful avenue for future empirical research. For example, it would be interesting to explore the role of three negative personality factors such as narcissism, Machiavellianism and psychopathy, referred to as the dark triad (Paulhus and Williams, 2002), in the context of knowledge sabotage behavior. *Fifth*, it is also vital to better understand how organizational policies and procedures facilitate or suppress undesirable knowledge sabotage behavior. For instance, practitioners would benefit from knowing how various pay structures, which may lead to the development of a highly competitive environment, contribute to counterproductive knowledge sabotage behavior. Afterward, it is important to develop a quantitative instrument to measure the presence of knowledge sabotage in organizations and use it within a nomological network explicating the antecedents and consequences of knowledge sabotage.

6. Conclusion

Despite making every attempt to remain neutral and, without bias, document the phenomenon of interest, every researcher has at least some preconceived notion about the nature of the future findings. Before embarking on an empirical investigation of knowledge sabotage, the author of the present study had spent over a decade contemplating its nature through observation and reading academic and practitioner literature. An initial assumption was that knowledge saboteurs are disgruntled employees who respond to a violation of explicit or implicit trust by their organizations and/or their managers and who intentionally try to inflict harm upon their organizations while clearly realizing the consequences of their action. After documenting the accounts of knowledge sabotage from the perspectives of both saboteurs (Serenko, 2019) and their victims (i.e. the present study), the proposition above has been completely refuted. Instead, knowledge sabotage is rarely driven by an injustice inflicted by an organization; instead, it is people's egoistic nature, a desire to engage in retaliatory behavior and general malevolence toward others, which drive knowledge sabotage in the contemporary organization. It seems that the stone age mentality, when the early humans engaged in severe competition for limited resources for the sake of mere survival, is still present in the contemporary workplace. In other words, as the attributes of contemporary society such as technologies, laws, management practices, the standard of living and so on, change, people's basic behavioral principles remain largely unaltered. Most importantly, both parties generally insist on their innocence: saboteurs believe that their victims provoked this malevolent action and fully deserve such treatment, whereas targets consider themselves fully guiltless. At the same time, knowledge sabotage has a drastic impact on the targets and costs their organizations dearly.

References

Alter, S. (2006), "Goals and tactics on the dark side of knowledge management", *Proceedings of the 39th HI International Conference on System Sciences*, IEEE, Kauai, HI.

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

Andersson, B.-E. and Nilsson, S.-G. (1964), "Studies in the reliability and validity of the critical incident technique", *Journal of Applied Psychology*, Vol. 48 No. 6, pp. 398-403.

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.

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.

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.

Bies, R.J. (2015), "Interactional justice: looking backward, looking forward", in Cropanzano, R.S. and Ambrose, M.L. (Eds), *The Oxford Handbook of Justice in the Workplace*, Oxford University Press, New York, NY, pp. 89-107.

Blau, P.M. (1964), *Exchange and Power in Social Life*, John Wiley, New York, NY.

Blau, G. and Andersson, L. (2005), "Testing a measure of instigated workplace incivility", *Journal of Occupational and Organizational Psychology*, Vol. 78 No. 4, pp. 595-614.

Bowling, N.A. and Beehr, T.A. (2006), "Workplace harassment from the victim's perspective: a theoretical model and meta-analysis", *Journal of Applied Psychology*, Vol. 91 No. 5, pp. 998-1012.

Bozeman, J. and Hershcovis, M.S. (2015), "The role of the victim and the perpetrator-victim relationship in understanding workplace aggression", in Paludi, M.A. (Ed.), *Bullies in the Workplace: Seeing and Stopping Adults Who Abuse Their co-Workers and Employees*, Praeger, Denver, CO, pp. 63-86.

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*, Vol. 6 No. 1, pp. 3-5.

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.

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.

Chao, J.M.C., Cheung, F.Y.L. and Wu, A.M.S. (2011), "Psychological contract breach and counterproductive workplace behaviors: testing moderating effect of attribution style and power distance", *The International Journal of Human Resource Management*, Vol. 22 No. 4, pp. 763-777.

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.

Cortina, L.M. and Magley, V.J. (2009), "Patterns and profiles of response to incivility in the workplace", *Journal of Occupational Health Psychology*, Vol. 14 No. 3, pp. 272-288.

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.

De Dreu, C.K.W. (2008), "The virtue and vice of workplace conflict: food for (pessimistic) thought", *Journal of Organizational Behavior*, Vol. 29 No. 1, pp. 5-18.

De Dreu, C.K.W. and Gelfand, M.J. (2008), "Conflict in the workplace: sources, functions, and dynamics across multiple levels of analysis", in Dreu, C.K.W.D. and Gelfand, M.J. (Eds), *The Psychology of Conflict and Conflict Management in Organizations*, Lawrence Erlbaum Associates, New York, NY, pp. 3-54.

Deutsch, M. (1973), *The Resolution of Conflict: Constructive and Destructive Processes*, Yale University Press, New Haven and London, Binghamton, N.Y.

Deutsch, M. (2012), "A theory of cooperation - competition and beyond", in Van Lange, P.A.M. and Kruglanski, A.W. and Higgins, E.T. (Eds), *Handbook of Theories of Social Psychology*, Sage, New Delhi, pp. 275-294.

Duffy, M.K., Ganster, D.C. and Pagon, M. (2002), "Social undermining in the workplace", *Academy of Management Journal*, Vol. 45 No. 2, pp. 331-351.

Ferraris, A., Erhardt, N. and Bresciani, S. (2019), "Ambidextrous work in smart city project alliances: unpacking the role of human resource management systems", *The International Journal of Human Resource Management*, Vol. 30 No. 4, pp. 680-701.

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.

Folger, R. and Konovsky, M.A. (1989), "Effects of procedural and distributive justice on reactions to pay raise decisions", *Academy of Management Journal*, Vol. 32 No. 1, pp. 115-130.

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.

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.

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 Promislo, M.D. (2010), "Unethical and unwell: decrements in well-being and unethical activity at work", *Journal of Business Ethics*, Vol. 91 No. 2, pp. 275-297.

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.

Greenwald, A.G., Poehlman, T.A., Uhlmann, E.L. and Banaji, M.R. (2009), "Understanding and using the implicit association test: III. Meta-analysis of predictive validity", *Journal of Personality and Social Psychology*, Vol. 97 No. 1, pp. 17-41.

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.

Henrich, J., Heine, S.J. and Norenzayan, A. (2010), "Most people are not WEIRD", *Nature*, Vol. 466 No. 7302, p. 29.

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.

Hershcovis, M.S. (2011), "Incivility, social undermining, bullying ... oh my!": a call to reconcile constructs within workplace aggression research", *Journal of Organizational Behavior*, Vol. 32 No. 3, pp. 499-519.

Hershcovis, M.S., Turner, N., Barling, J., Arnold, K.A., Dupré, K.E., Inness, M., LeBlanc, M.M. and Sivanathan, N. (2007), "Predicting workplace aggression: a meta-analysis", *Journal of Applied Psychology*, Vol. 92 No. 1, pp. 228-238.

Indvik, J. and Johnson, P.R. (2009), "Liar! liar! your pants are on fire: deceptive communication in the workplace", *Journal of Organizational Culture, Communications and Conflict*, Vol. 13 No. 1, pp. 1-8.

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.

Jehn, K.A. (1995), "A multimethod examination of the benefits and detriments of intragroup conflict", *Administrative Science Quarterly*, Vol. 40 No. 2, pp. 256-282.

Jehn, K.A., Rispens, S. and Thatcher, S.M. (2010), "The effects of conflict asymmetry on work group and individual outcomes", *Academy of Management Journal*, Vol. 53 No. 3, pp. 596-616.

Johnson, P.R. and Indvik, J. (2001), "Rudeness at work: Impulse over restraint", *Public Personnel Management*, Vol. 30 No. 4, pp. 457-465.

Joseph, R. (1992), *The Right Brain and the Unconscious: Discovering the Stranger Within*, Plenum Publishing, New York, NY.

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.

Kelly, H.H., *et al* (1972), "Attribution in social interaction", in Jones, E.E., Kanouse, D.E., Kelly, H.H. (Eds), *Attribution: Perceiving the Causes of Behavior*, General Learning Press, Morristown, N.J., pp. 1-27.

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.

Koenemann-Belliveau, J., Carroll, J.M., Rosson, M.B. and Singley, M.K. (1994), "Comparative usability evaluation: critical incidents and critical threads", *Proceedings of the ACM Conference on Human Factors in Computing Systems*, The ACM Press, Boston, MA.

Krieger, N., Waterman, P.D., Hartman, C., Bates, L.M., Stoddard, A.M., Quinn, M.M., Sorensen, G. and Barbeau, E.M. (2006), "Social hazards on the job: workplace abuse, sexual harassment, and racial discrimination - A study of black, Latino, and white low-income women and men workers in the United States", *International Journal of Health Services*, Vol. 36 No. 1, pp. 51-85.

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

Kwak, D.-H., Holtkamp, P. and Kim, S.S. (2019), "Measuring and controlling social desirability bias: applications in information systems research", *Journal of the Association for Information Systems*, Vol. 20 No. 4, pp. 317-345.

Landers, R.N. and Callan, R.C. (2014), "Validation of the beneficial and harmful work-related social media behavioral taxonomies development of the work-related social media questionnaire", *Social Science Computer Review*, Vol. 32 No. 5, pp. 628-646.

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.

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.

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*, Vol. 17 No. 2, pp. 203-212.

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

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. and Konno, N. (1998), "The concept of 'ba': building a foundation for knowledge creation", *California Management Review*, Vol. 40 No. 3, pp. 40-54.

Palvia, P., Jacks, T., Ghosh, J., Licker, P., Romm-Livermore, C., Serenko, A. and Turan, A.H. (2017), "The World IT Project: history, trials, tribulations, lessons, and recommendations", *Communications of the Association for Information Systems*, Vol. 41 No. 1, pp. 389-413.

Paulhus, D.L. and Williams, K.M. (2002), "The dark triad of personality: narcissism, Machiavellianism, and psychopathy", *Journal of Research in Personality*, Vol. 36 No. 6, pp. 556-563.

Payne, H.J. (2008), "Targets, strategies, and topics of deception among part-time workers", *Employee Relations*, Vol. 30 No. 3, pp. 251-263.

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.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. and Podsakoff, N.P. (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903.

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, pp. 367-395.

Reich, T.C. and Hershcovis, M.S. (2015), "Observing workplace incivility", *Journal of Applied Psychology*, Vol. 100 No. 1, pp. 203-215.

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.

Robinson, S.L., Kraatz, M.S. and Rousseau, D.M. (1994), "Changing obligations and the psychological contract: a longitudinal study", *Academy of Management Journal*, Vol. 37 No. 1, pp. 137-152.

Ronan, W.W. and Latham, G.P. (1974), "The reliability and validity of the critical incident technique: a closer look", *Studies in Personnel Psychology*, Vol. 6 No. 1, pp. 53-64.

Rousseau, D.M. (1989), "Psychological and implied contracts in organizations", *Employee Responsibilities and Rights Journal*, Vol. 2 No. 2, pp. 121-139.

Semerci, A.B. (2019), "Examination of knowledge hiding with conflict, competition and personal values", *International Journal of Conflict Management*, Vol. 30 No. 1, pp. 111-131.

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. (2019), "Knowledge sabotage as an extreme form of counterproductive knowledge behavior: conceptualization, typology, and empirical demonstration", *Journal of Knowledge Management*, Vol. 23 No. 7, pp. 1260-1288.

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.

Serenko, A. and Turel, O. (2019), "A dual-attitude model of system use: the effect of explicit and implicit attitudes", *Information & Management*, Vol. 56 No. 5, pp. 657-668.

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.

Shulman, D. (2008), "More lies than meet the eyes: organizational realities and deceptions in nonprofit organizations", *International Journal of Not-for-Profit Law*, Vol. 10 No. 2, pp. 5-14.

Skarlicki, D.P. and Folger, R. (1997), "Retaliation in the workplace: the roles of distributive, procedural, and interactional justice", *Journal of Applied Psychology*, Vol. 82 No. 3, pp. 434-443.

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

Totterdell, P., Hershcovis, M.S., Niven, K., Reich, T.C. and Stride, C. (2012), "Can employees be emotionally drained by witnessing unpleasant interactions between coworkers? A diary study of induced emotion regulation", *Work & Stress*, Vol. 26 No. 2, pp. 112-129.

Tripp, T.M. and Bies, R.J. (2009), *Getting Even: The Truth about Workplace Revenge – and How to Stop It*, Jossey-Bass, San Francisco.

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.

Tsui, A.S., Pearce, J.L., Porter, L.W. and Tripoli, A.M. (1997), "Alternative approaches to the employee-organization relationship: does investment in employees pay off?", *Academy of Management Journal*, Vol. 40 No. 5, pp. 1089-1121.

Vartia, M.A.-L. (2001), "Consequences of workplace bullying with respect to the well-being of its targets and the observers of bullying", *Scandinavian Journal of Work, Environment & Health*, Vol. 27 No. 1, pp. 63-69.

Weiner, B., Frieze, I., Kukla, A., Reed, L., Rest, S., Rosenbaum, R.M. (1972), "Perceiving the causes of success and failure", in Jones, E.E., Kanouse, D.E., Kelly, H.H. (Eds), *Attribution: Perceiving the Causes of Behavior*, General Learning Press, Morristown, N.J., pp. 95-120.

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

Appendix 1. The questionnaire

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

(Note: The order of the situations below was randomized for each respondent to avoid order bias.)

Situation 1

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

During your entire working career, how many times have you experienced a situation similar to the one described above? (Options: 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 and/or your organization (i.e., it was the most critical). If you have never experienced a similar situation, proceed to Situation 2:

- Explain *in detail* what happened.
- Who did this person act against? (check all that apply – options: you; your organization; someone else)
- Why did he/she do this to you?
- What impact did it have on the task you were working on?
- Did you change your attitude and/or behavior toward this person? If yes, please elaborate.
- Did you change your attitude and/or behavior toward this organization? If yes, please elaborate.
- Did you ever try to retaliate against this person by providing him/her with wrong information, advice, a document, or a recommendation? If yes, please elaborate.
- Who do you think is responsible for what happened? (check all that apply – options: the person who did it to me; the organization; the manager; myself; someone else)
- How often did similar incidents take place in this organization? (options: never; very rarely; rarely; occasionally; sometimes; often; very often)
- Did you report this incident to anyone? If yes, who did you report it to? What happened after that?

Situation 2

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

During your entire working career, how many times have you experienced a situation similar to the one described above?

Out of all situations similar to the situation described above, recall the one that had the most dramatic impact on you and/or your organization (i.e., it was the most critical). If you have never experienced a similar situation, proceed to demographics.

(The same questions as in Situation 1.)

Appendix 2. The final codebook

Table AI The final codebook

Second-order themes	*First-order themes*
Type of knowledge	Tangible: training manuals, computer files, documentation, reports, notes and templates
	Intangible: verbal advice, recommendations and tips
Target	The person: colleague, subordinate and manager
	The organization
	The third party
Driver	Gratification: personal career, personal gain and mistake cover-up
	Retaliation against other employees because of: envy, grudge and personal incompatibility
	Malevolent personality: malevolence toward others, poor attitude, playing jokes on others and psychological issues
	Organization-related: saving money
Impact	On the person: lower job efficiency (time loss and missing work/being late); psychological impact (public humiliation and stress/pressure); career impact (official reprimand, impeded career, voluntary resignation and wrongful dismissal); and direct financial impact
	On the organization: failed/delayed project, time loss, direct financial impact, being out of stock, loss of clients, being understaffed and lower output quality
	On the third party: inconvenience, financial impact and emotional/physical suffering
Attribution of responsibility	Myself
	The saboteur
	The manager
	The organization
Changes in attitude	Lack of trust
	Negativity
Changes in behavior	Avoidance
	Lack of knowledge sharing
	Hostility
	Reduced work effort
Incident reporting (i.e. complained to)	The manager/superior
	Other employees
	The human resources office
	The union
Reason for not reporting the incident	Useless (because no action against the saboteur will be taken)
	Lack of poof
	Withdrawal (did not want to deal with the situation any longer)
Action against saboteurs	Fired from the organization
	Formally reprimanded
	Transferred to another division/department within the organization

About the author

Dr Alexander Serenko is an Associate Professor of Management Information Systems in the Faculty of Business and IT, University of Ontario Institute of Technology and a Lecturer in the Faculty of Information, University of Toronto. Dr Serenko holds a PhD in Management Information Systems from McMaster University. His research interests pertain to scientometrics, knowledge management, technology addiction, and implicit cognitive processes. 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, and his works have received more than 7,000 citations. Alexander has also won six Best Paper awards at Canadian and international conferences. In 2018, he was ranked one of the most productive and influential academics in the knowledge management discipline. Alexander Serenko can be contacted at: a.serenko@utoronto.ca

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com