Received: 9 September 2019 | Revised: 28 July 2020 | Accepted: 2 August 2020

DOI: 10.1002/joom.1116

RESEARCH ARTICLE

WILEY

Spillover effects of information leakages in buyer–supplier–supplier triads

Leopold Ried[1] | **Stephanie Eckerd**[2] | **Lutz Kaufmann**[1] | **Craig Carter**[3]

[1]WHU – Otto Beisheim School of Management, Vallendar, Germany

[2]Haslam College of Business, University of Tennessee, Knoxville, Tennessee

[3]W.P. Carey School of Business, Arizona State University, Tempe, Arizona

Correspondence
Stephanie Eckerd, Haslam College of Business, University of Tennessee, Knoxville, TN
Email: seckerd@utk.edu.

Handling Editor: Gopesh Anand

Abstract

Information leakages—the unauthorized sharing of an organization's information with another organization—are a growing concern in today's supply chains, but remain relatively underexplored. Drawing on attribution theory and observational learning, our research investigates inter-organizational information leakages from a network perspective. We assess the spillover effects of opportunistic and inadvertent information leakages between an *OFFENDER* organization and a *VICTIM* organization on the relationship between the *OFFENDER* and a nonpartisan *OBSERVER*. We consider the roles of integrity- and ability-based trust, as well as operational similarity between the organizations. We conducted scenario-based experiments with 181 sales practitioners recruited via MTurk and supplemented those results with post hoc interviews. Our results show clear spillover effects: The *OBSERVER*'s willingness to share information with the *OFFENDER* decreases significantly after any type of information leakage between the *OFFENDER* and the *VICTIM,* but more so for opportunistic leakages. Integrity-based trust mediates the relationship between intentionality and information sharing willingness. We also find indications of an unexpected collateral damage effect in that to some extent, both trust dimensions decrease in both forms of information leakage. Further, for opportunistic information leakages, the *OBSERVER*'s willingness to share information with the *OFFENDER* decreases more when *OBSERVER* and *VICTIM* are operationally similar.

KEYWORDS

attribution theory, information leakage, network, observational learning, opportunism, scenario-based experiments, spillover, trust

1 | INTRODUCTION

Information sharing processes within supply chains create well-established benefits for the organizations involved, such as increased commitment and trust (Nyaga, Whipple, & Lynch, 2010) and enhanced supply chain collaboration (Cao & Zhang, 2011; Sheu, Yen, & Chae, 2006). However, once shared, the potential arises for *information leakages*—the unauthorized sharing of information with other members of the supply chain. For example, general motors (GM) shared a key supplier's confidential product design information with other suppliers to obtain more favorable purchase prices (Anand & Goyal, 2009). When confidential information is leaked to unauthorized parties, as in the GM example, the leak ultimately weakens the victim's competitive position through the exposure of proprietary product details and production processes (Kovach, Pruett, Samuels, &

Duvall, 2004), sales and demand data (Li, 2002), strategy plans (Pandey, Garg, & Shankar, 2010), and best practices (Hoecht & Trott, 2006). In addition, the number of information leakage events in recent years has grown and represents a critical challenge for practitioners (Rogers, Benjamin, & Gopalakrishnan, 2018). The resulting tension between the potential benefits of information sharing and vulnerabilities stemming from information leakages calls for research on when organizations are—and when they are not—willing to share sensitive information, given the confidentiality issues and concerns caused by information leakages.

We formally define information leakages as the "revelation of confidential information to an unauthorized party" (Zhang, Cao, Wang, & Zeng, 2012, p. 1351), which might either happen inadvertently or be opportunistically motivated.[1] Inadvertent information leakages are unintentional or accidental. They have frequently been studied from the perspective of how or when an organization's own employees leak internal confidential information to outsiders—for instance, because of enthusiasm about the organization's activities (Ritala et al., 2015) or because of ambiguities about which information employees are allowed to share with outsiders (Husted & Michailova, 2010). Inadvertent information leakages caused by *outside organizations* have been explored to a much lesser extent (Massimino, Gray, & Lan, 2018).

Opportunistic information leakages are regarded as intentional or deliberate, consistent with opportunism's definition as "self-interest seeking with guile" (Williamson, 1985, p. 47). Opportunistic information leakages can arise from a variety of sources: Internal breaches might involve leaking of confidential information by the organization's own employees to outsiders (Delerue & Lejeune, 2010), and external breaches might involve sharing of sensitive data with unauthorized organizations by partner organizations (Kong et al., 2017). As noted by Massimino et al. (2018), most research in operations and supply chain management (OSCM) acknowledges different causes of information leakages (i.e., both inadvertent and opportunistic), but rarely is the difference made explicit in either theorizing or empirical analysis. This lack of distinction suggests that most literature to date has considered inadvertent and opportunistic information leakages as equally predictive on outcomes, such as an organization's willingness to share information. We challenge this assumption, drawing on and extending attribution theory to explain differences in the effects of inadvertent versus opportunistic information leakages on the willingness to share information.

Moreover, much of what we know about information leakages pertains directly to the buyer–supplier dyad, for example designing contracts that might exacerbate or mitigate information leakages (Anand & Goyal, 2009; Kong, Rajagopalan, & Zhang, 2013). However, organizations in the broader network may observe events in their environment and apply what they learn from those observations to their own interactions. In the previously noted example involving GM, suppliers other than the victim might learn about GM's offense, and those observant suppliers might change the way they share information with GM as a result. In other words, a spillover effect associated with information leakage might arise. We define a *spillover* as occurring when an entity merely *observes* an event and that observation affects the entity's behavior in some way. Hora and Klassen (2013) similarly define spillovers and assess them in their investigation of factors that prompt risk managers to seek out knowledge about another organization's operational losses (i.e., to engage in learning through spillovers). We extend this conceptualization to understand how observational learning in the context of information leakages has worked, and how spillovers affect supply chain relationships from a network perspective, which are both relatively underinvestigated areas.

Our work departs from previous literature by adopting a network perspective and drawing on the concepts of inter-organizational observational learning and attribution theory to posit *why* observer organizations might be differentially affected by information leakages within the supply network, and *how* this changes the observer's behavior. Networks consist of triads, which can be regarded as "the fundamental building blocks of a network" (Choi & Wu, 2009, p. 8). Specifically, we consider a triadic supply network comprising one buyer and two suppliers (Choi & Wu, 2009). In this context, one supplier (referred to as the *OBSERVER*) learns about an information leakage caused by the buyer (referred to as the *OFFENDER*) regarding the other supplier (referred to as the *VICTIM*), as depicted in Figure 1.

This triadic supply network structure leads to our study's primary research question: What is the differential effect of inadvertent versus opportunistic information leakages on an *OBSERVER's* willingness to share information with an *OFFENDER*? We also examine whether this effect is mediated by a reduction in the *OBSERVER's* integrity- and ability-based trust in the *OFFENDER*, as the nature of events informs trust evaluations (Hill, Eckerd, Wilson, & Greer, 2009) and trust is foundational to a wide range of relational behaviors, including information sharing (Ebrahim-Khanjari, Hopp, & Iravani, 2012). Moreover, we account for the moderating effect of the degree of similarity between *VICTIM* and *OBSERVER* because literature on observational learning suggests that the level of *similarity* between entities is a

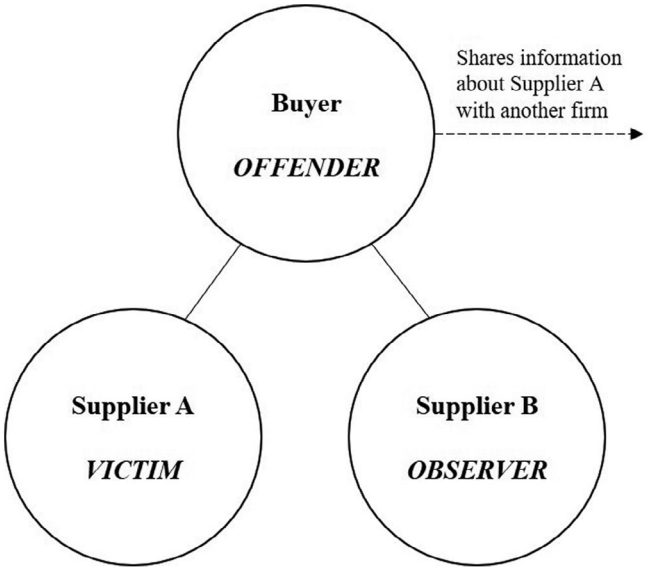

FIGURE 1 Network roles

key factor when learning from others (Baum, Li, & Usher, 2000; Haunschild & Miner, 1997; Hora & Klassen, 2013).

We examined our research question by conducting scenario-based experiments with a final sample of 181 sales practitioners recruited via MTurk. We supplemented our results with post hoc interviews with a different sample of sales practitioners spanning different countries. Leveraging attribution theory and observational learning, we derive four major findings offering valuable implications for theory. First, the *OBSERVER*'s information sharing willingness with the *OFFENDER* decreases significantly after any type of information leakage between the *OFFENDER* and the *VICTIM*. This supports the theorized spillover effect and shows the extent of negative outcomes of information leakages in supply networks. Second, information leakages having opportunistic attributions lead to more severe consequences, justifying a separation of causalities when exploring confidentiality issues in future research. Third, integrity-based trust significantly mediates the relationship between intentionality and information sharing willingness in *both* forms of information leakage; we further find indications of a collateral damage effect, in that to some extent ability-based trust decreases in *both* forms of information leakage. This finding was unexpected in light of developments surrounding hierarchically restrictive schema (Reeder & Brewer, 1979), and we thereby contribute an improved understanding of the breadth of the effects that information leakages have on trust in network relationships. Fourth, when an *OBSERVER* sees an opportunistic information leakage, the *OBSERVER's* information sharing willingness with the *OFFENDER* decreases more when the *OBSERVER* and the *VICTIM* are operationally similar than when they are operationally different from each other. However, the effect of operational similarity is bounded: It does not play a role when the information leakage stems from inadvertent causes.

In practice, *OFFENDERs* should be aware that even inadvertent information leakages can have far-reaching detrimental effects. Our findings provide a good argument for increasing information integrity efforts—a challenge that continues to elude practitioners (Massimino et al., 2018; Speier, Whipple, Closs, & Voss, 2011). *OBSERVERs* should also become certain of the *OFFENDER's* intention behind an information leakage, which our findings show lead to significantly different levels of information sharing willingness.

2 | THEORETICAL BACKGROUND AND HYPOTHESES

2.1 | Theoretical underpinnings

Organizations acquire knowledge over time, which serves as a valuable resource that can ultimately create substantial competitive advantage (March, 1991; Moorman & Miner, 1997; Sinkula, Baker, & Noordewier, 1997). One way to accumulate this knowledge is through observational learning, frequently referred to as vicarious learning (Burke, Tobler, Baddeley, & Schultz, 2010). Such learning is defined as behaviors derived from the observations of others' behavior (Bandura, 1971). Hence, organizations learn from observations in their broader environment and subsequently apply these lessons in their actions. Rooted in Bandura's social learning theory, observational learning adheres to a process of sense-making, which requires a cognitive understanding of the actions observed (i.e., stimuli) and their associated responses (Bandura, 1971). An important element of this process, in accordance with attribution theory, deals with how individuals assign causation to an observed event—that is, *why* the event happened (Weiner, 1985).

Previous studies in OSCM indicate that the attribution of a transgression can play a major role in predicting the response processes of counterparties (Eckerd, Hill, Boyer, Donohue, & Ward, 2013; Hora & Klassen, 2013). Attribution theory traditionally is based on three dimensions: locus of causality, controllability, and stability (Fiske & Taylor, 1991; Weiner, 1986, 1995). Locus of causality describes who or what the observer determines is the responsible source for the incident; controllability evaluates the degree to which the source would have been able to avoid the event; and stability covers the time

aspect through an assessment of whether the action's driver is temporary or permanent (Mir, Aloysius, & Eckerd, 2016). In our research, we assume these three traditional dimensions as given, which will be explained further in Subsection 3.1. In a departure from recent OSCM research employing attribution theory (Hartmann & Moeller, 2014; Polyviou, Rungtusanatham, Reczek, & Knemeyer, 2018), we introduce and evaluate the *intentionality* dimension of attribution—a dimension that has received scant empirical attention (Harvey, Madison, Martinko, Crook, & Crook, 2014). We follow Harvey et al.'s conceptualization of intentionality as "the extent to which an outcome is attributed to deliberate as opposed to unintentional action. As the name suggests, attributions of intentionality occur when a perceiver believes that an outcome was caused by the deliberate and informed actions of another" (2014, p. 136). Using this lens, we can account for actions that are well-intentioned but that nonetheless generate unanticipated outcomes. This conceptualization captures an important, but often overlooked, dimension of events that is critical to the sense-making process for determining attribution. Indeed, recent OSCM research suggests that intentional and unintentional supply chain events might be handled very differently (DuHadway, Carnovale, & Hazen, 2019; Speier et al., 2011), emphasizing the importance of this dimension for incidents affecting the supply chain.

2.2 | Inadvertent versus opportunistic information leakages

The various benefits of inter-organizational information sharing between supply chain partners have long been established by researchers, illustrating the potential for higher quality performance (Carter & Miller, 1989), facilitation of joint innovations (Ritala et al., 2015), and problem solving with regard to materials and designs (Carr & Pearson, 1999; Giunipero, 1990). Undoubtedly, information sharing can be beneficial and is often necessary; however, it also poses potential risks to both buyers and suppliers. For instance, previous research has underscored the danger of retailers providing unreliable demand forecast information to their suppliers (Spiliotopoulou, Donohue, & Gürbüz, 2016), a factor that can be especially exacerbated when considering global supply chain partners (Özer, Zheng, & Chen, 2011). Retailers are prone to risk as well when sharing information, since suppliers may use the information to circumvent retailers and sell directly to end users (Huang, Guan, & Chen, 2018). These contributions have provided valuable insights into the potential downsides connected to information sharing within the supply chain. However, one still relatively underexplored but increasingly relevant hazard inherent to information sharing constitutes that of information leakages within the wider supply network.

Information leakages can be inadvertent (i.e., unintentional) or opportunistic (i.e., intentional) behavior. Inadvertent information sharing between organizations has been facilitated with the near-universal use of e-mail, despite organizations' prevention efforts (Zilberman, Katz, Shabtai, & Elovici, 2013). Digitalized communication channels allow the instant exchange of information, which does not leave much time for spotting mistakes in the process. E-mails containing confidential information can easily be sent to the wrong recipient simply because of typing errors or misplaced clicks. Conversely, opportunistically motivated leakage concerns the deliberate sharing or selling of a partner organization's confidential information, such as in the GM example from the Introduction. We argue that regardless of the attribution—whether inadvertent or opportunistic—the *OBSERVER's* willingness to share information with the *OFFENDER* should decrease after learning about the information leakage event; this decline is a spillover effect. No matter the rationale, the fact remains that sensitive information—such as product or process technologies—has been shared through the *OFFENDER's* actions, resulting in potential losses for the *VICTIM* (Massimino et al., 2018). Observational learning suggests that managers will try to avoid similar potential losses and adjust their actions accordingly. This "avoidance learning," as a specific form of observational learning (Krypotos, Effting, Kindt, & Beckers, 2015), occurs in inter-organizational relationships and is driven by the fear that sharing business-critical information allows for potential exploitation by counterparties (Ahmad, Bosua, & Scheepers, 2014).

Although we expect to find overall decreases in the *OBSERVER's* willingness to share information upon learning of an information leakage within the network, we expect the *magnitude* to differ depending on the attribution of the *OFFENDER's* intentionality. Indeed, psychological research at the interpersonal level suggests that intentional violations cause observers to assign greater responsibility to the *OFFENDER*, and they trigger more negative and harsher moral judgments by others than similar unintentional events (Guglielmo & Malle, 2010; Parkinson & Byrne, 2018). Researchers have long acknowledged that employees' behaviors are frequently perceived as representative of the entire organization to outsiders—for example, when it comes to brand impressions after a single employee's actions (Wentzel, 2009). Whereas opportunistic leakages necessitate a high degree of consciousness, inadvertent leakages

lack a calculating element because the actor was not purposeful. In the case of inadvertent wrongdoing, culpability is mitigated and others assign less blame for the event to the entity responsible (Simester, 2005). When tied back to the observational learning literature, we anticipate that these attributions surrounding intentionality will inform subsequent reactions. As such, we argue that the attribution is stronger in an opportunistic event, leading to a harsher judgment and a stronger reaction by the *OBSERVER*, as characterized by an even lower information sharing willingness than in inadvertent circumstances. Thus, we hypothesize the following:

HYPOTHESIS 1a *An OBSERVER's willingness to share information with an OFFENDER decreases after that OFFENDER is known to have inadvertently shared confidential information about a VICTIM.*

HYPOTHESIS 1b *An OBSERVER's willingness to share information with an OFFENDER decreases after that OFFENDER is known to have opportunistically shared confidential information about a VICTIM.*

HYPOTHESIS 1c *An OBSERVER's willingness to share information with an OFFENDER decreases to a greater extent after that OFFENDER is known to have opportunistically, rather than inadvertently, shared confidential information about a VICTIM.*

2.3 | Role of trust

One of the key relational mechanisms used to govern inter-organizational exchange is trust, which has long been recognized as a crucial determinant for successful business relationships (Johnston, McCutcheon, Stuart, & Kerwood, 2004; Mohr & Spekman, 1994; Morgan & Hunt, 1994). Researchers have determined various antecedents of trust in the literature, including the role of historical reciprocity between buyers and suppliers (Cai, Jun, & Yang, 2010; Gulati, 1995; Gulati & Sytch, 2008). Trust is also key to inter-organizational information sharing as an outcome (Devaraj, Vaidyanathan, & Mishra, 2012; Flynn, Koufteros, & Lu, 2016), particularly given the sensitive nature of some types of information and the associated risk of a leakage. Li and Lin (2006) conclude that "trust reduces the fear of information disclosure" (p. 1644), and Hoecht and Trott (2006) determine in their study that trust can be an even more relevant factor for managing inter-organizational information leakage risks than bureaucratic control and legal contracts.

We suggest that trust also is a key mechanism at play in interpretations of and responses to an *OFFENDER's* behavior following an information leakage, even though the *OBSERVER* is not directly involved in or affected by it. We argue that the focal supplier (i.e., the *OBSERVER*) sees the actions of the *OFFENDER* and integrates this learning into the perception of trust in the *OFFENDER*. Previous literature has established three main trust dimensions: ability-based trust, integrity-based trust, and benevolence-based trust (Mayer & Davis, 1999); however, work in the inter-organization domain has largely omitted benevolence trust from consideration because it is less applicable to these relationships (e.g., Connelly, Crook, Combs, Ketchen, & Aguinis, 2018). We follow the guidance of Connelly and colleagues and consider only ability- and integrity-based trust in this research (Connelly et al., 2018).

Ability-based trust, which we argue to be relevant when considering inadvertent information leakages, addresses the confidence a party has in the skills, knowledge, and competence of its partner. When a buyer exhibits a lack of these skills, such as by inadvertently leaking a supplier's proprietary information to an outside party, the buyer risks damage to its ability-based trustworthiness because the *OBSERVER* might project this carelessness onto the buyer's overall ability. Interestingly, prior research on hierarchically restrictive schema suggests that such projection should not happen as the result of a single ability-based transgression (Reeder & Brewer, 1979); however, this literature is grounded primarily in an interpersonal context. Ability-based negative events in inter-organizational relationships tend to involve more damaging consequences and monetary losses, which we argue results in stronger judgments after a *single* negative event that involves the leakage of confidential information. As such, we suggest that ability-based trust mediates the relationship between an inadvertent information leakage in the supply network and the *OBSERVER's* willingness to share information with the *OFFENDER* in the future. We do not expect ability-based trust to be a factor when considering opportunistic behavior; instead, we anticipate that this relationship is explained via integrity-based trust.

Integrity-based trust addresses the extent to which norms and values are shared across parties (Mayer & Davis, 1999). When the *OFFENDER* acts opportunistically, the action sends a signal to other network members of an unacceptable standard of *behavior*. This behavior, as described previously, is intentional and presumably supersedes any questions of ability of the *OFFENDER*. Moreover, although the negative event might have been targeted at a different supplier (i.e., the *VICTIM*), the motivation for the *OFFENDER's* action suggests to the *OBSERVER* a more overarching destructive behavior. This effect is consistent with the notion of hierarchically

restrictive schema (Reeder & Brewer, 1979), in which even a single integrity violation is a strong indication of a party's integrity overall. As such, the *OBSERVER's* integrity-based trust in the *OFFENDER* is posited to decline because of the *OBSERVER's* fear of a similar fate in the future. We therefore argue that integrity-based trust mediates the relationship between an opportunistic information leakage in the supply network and the *OBSERVER's* willingness to share information with that *OFFENDER* in the future. We propose two further hypotheses:

HYPOTHESIS 2a *An OBSERVER's willingness to share information with an OFFENDER that inadvertently shared confidential information about a VICTIM is mediated by the OBSERVER's ability-based trust in that OFFENDER.*

HYPOTHESIS 2b *An OBSERVER's willingness to share information with an OFFENDER that opportunistically shared confidential information about a VICTIM is mediated by the OBSERVER's integrity-based trust in that OFFENDER.*

2.4 | Operational similarity

As noted, perceptions of trust are expected to mediate the relationship between an information leakage and willingness to share information; meanwhile, the *operational similarity* between the *OBSERVER* and the *VICTIM* organizations is expected to moderate the relationship between intentionality and trust. Previous organizational learning studies demonstrate a positive association between the degree of similarity and the actual extent of learning from other organizations (Baum et al., 2000; Thornton & Thompson, 2001). The underlying rationale suggests that the lessons learned via observation of comparable organizations can be applied more easily to one's own organization (Baum et al., 2000). This connection proves useful for organizations in that, when their ability to learn from direct experience is hampered, they still can benefit from observing the actions and experiences of other comparable organizations (Haunschild & Miner, 1997). For example, Baum et al. (2000) examined the facility location decisions of nursing home chains and found that they tended to follow other chains' acquisition behavior. In another study concerning the commercial banking industry, researchers showed that banks learned from the near-failure experiences of other institutions, and that this learning effect was stronger when derived from financial institutions of similar structure (Kim & Miner, 2007).

Many of the perceptions and behaviors described in previous organizational learning studies can be reconciled with the concept of group identity, which describes the extent to which one feels belonging to a group (i.e., in-group status) versus not belonging to a group (i.e., out-group status) (Corsten, Gruen, & Peyinghaus, 2011). Common identities create trust in inter-organizational relationships (Gulati & Sytch, 2008; Ireland & Webb, 2007). Importantly, studies suggest that the perceived degree of identification with a group drives emotional and cognitive mechanisms following events that affect the group (Smith, Seger, & Mackie, 2007; Urda & Loch, 2013). In addition, group identity substantively influences perception and interpretation of events (Menges & Kilduff, 2015). Taken together, the evidence strongly supports the importance of similarity in observational learning and resulting perceptions.

One particularly relevant dimension of similarity in the supply chain context is that of operational similarity, which "emanates from utilizing similar processes, producing similar products, or delivering similar services" (Hora & Klassen, 2013, p. 54). Hora and Klassen (2013) found that organizations with high operational similarity engaged in greater knowledge acquisition when learning about and from an operational loss of another organization. This effect occurs because managers face less causal ambiguity and can more easily identify, examine, monitor, and learn from other organizations' loss events when these organizations are operationally similar. We therefore adopt the lens of operational similarity in this study, arguing that the *OBSERVER* of an information leakage should perceive a more salient group identity with the *VICTIM* if that *VICTIM* supplies a product similar to that of the *OBSERVER*. This shared group identity between the *OBSERVER* and *VICTIM* is expected to strengthen observational learning and the perceived transferability of events between *VICTIM* and *OBSERVER*—that is, to more strongly affect the *OBSERVER's* trust towards the *OFFENDER* due to the fear of a similar fate in the future.

Building on our arguments surrounding the mediating roles of integrity- and ability-based trust in the relationship between intentionality and information sharing willingness, we therefore assume a moderated mediation relationship, where operational similarity as the moderator affects the magnitude of the respective mediating process at hand. We summarize the assumed moderation effect of operational similarity into the following hypothesis:

HYPOTHESIS 3 *The degree of operational similarity between a VICTIM and an OBSERVER is negatively associated with the OBSERVER's trust towards the OFFENDER after an information leakage event.*

The proposed research model of this study is depicted in Figure 2.

3 | METHODOLOGY

3.1 | Experimental design and procedures

We tested our hypotheses using a scenario-based role-playing experiment. We used a 2 (Intentionality: inadvertent versus opportunistic) x 2 (Operational Similarity: similarity versus dissimilarity) mixed experimental design, comprising the collection of both within- and between-participant data. Between-participant data were gathered through the random allocation of participants to one of the four treatments and served as the main data for analyzing H1c, H2a, H2b, and H3. Within-participant data were collected by measuring the trust construct and the information sharing willingness construct both ex ante and ex post the information leakage event. This provided the data to analyze H1a and H1b. The within-participant data also served as an additional robustness test to verify that participants did not systematically respond in different ways before any induced treatment.

The focal organization of this study is the *OBSERVER*, one of two suppliers in a buyer–supplier–supplier triad. All research participants took on the role of the *OBSERVER* during the experiment (i.e., they were asked to act as the representative of the observing supplier organization). Data collection involved the following four steps: First, participants read an introduction scenario describing the general situation; this text was consistent across all treatments. Second, they answered questions assessing baseline levels of trust and information sharing willingness, before any treatment was administered. Third, after we collected these baseline measures, we randomly assigned participants to a treatment scenario involving information leakage by the *OFFENDER*. Each participant received one version of the four different treatment scenarios. In the *inadvertent* treatment, the leakage occurred because the *OFFENDER* unintentionally sent a confidential e-mail with sensitive information about the *VICTIM* to the wrong recipient, and in the *opportunistic* treatment, the *OFFENDER* deliberately leaked the same sensitive information about the *VICTIM* to a prospective industry customer. In the *operational similarity* treatment, the *VICTIM* and *OBSERVER* organizations were manufacturers of drone and smartphone batteries, respectively. In the *operational dissimilarity* treatment, the *VICTIM* was a supplier of drone cameras, whereas the *OBSERVER* was a supplier of smartphone batteries. We controlled for the relationship between the *VICTIM* and the *OBSERVER* by clearly stating that the two firms had no pre-existing relationship with each other (neither cooperative nor adversarial) and that they neither were current competitors nor had plans to enter each other's markets in the future. We therefore exclude the possibility of the *OBSERVER* benefitting from the leaked information or the leakage itself in two ways: (a) The *OBSERVER* does not gain access to the information, and (b) *VICTIM* and *OBSERVER* share no relationship with each other, ruling out potential competitive advantages for the *OBSERVER* from the event. Furthermore, we control for symmetrical power between *OFFENDER* and *OBSERVER*, as the *OBSERVER's* ability to reduce information sharing might be hampered in an asymmetric power relationship in which the *OBSERVER* depends highly on the buyer, based on arguments regarding power-opportunism interplays (Handley & Benton Jr., 2012; Handley, de Jong, & Benton Jr., 2019). Fourth, after reading the treatment vignette,

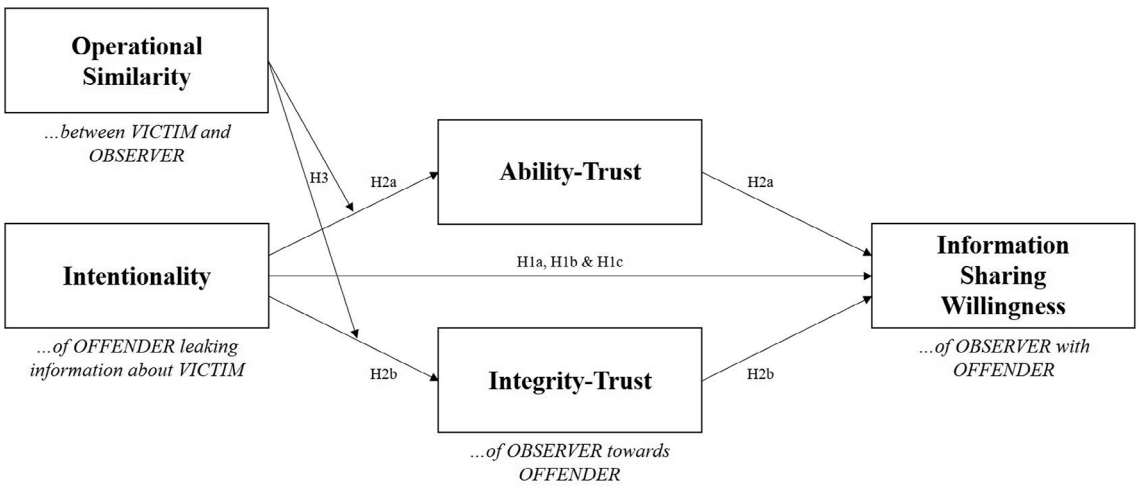

FIGURE 2 Research model

participants once again responded to questions about trust and information sharing willingness. They also responded to basic demographic questions, as well as to realism and manipulation checks.

As stated previously, we assume the three traditional dimensions of attribution theory—causality, controllability, and stability (Fiske & Taylor, 1991; Weiner, 1986, 1995)—as given in this study. First, the buyer is the source of the leakage (i.e., locus of causality). Second, the buyer maintains responsibility (i.e., controllability) for the action, since a different decision could have been made: in the opportunistic case not to be opportunistic, and in the inadvertent incident to be more diligent by putting individual safety measures in place such as to use encrypted data transfer for highly confidential information with only the appropriate receiver holding the digital key. Third, the event is a one-time incident in both leakage types, as the buyer never broke any written or verbal commitment with the supplier in the past (i.e., stability); therefore both leakage incidents are framed in the same historical setting and with no indication of any one leakage to be of a more permanently driven nature than the other (Oflaç, Sullivan, & Baltacioğlu, 2012).

We undertook two pilot studies prior to the main data collection to confirm the realism, clarity, and conciseness of the experimental vignettes and to improve them as appropriate (Wason, Polonsky, & Hyman, 2002). The first pilot study was conducted with 222 undergraduate students from a European business school and the second with 39 undergraduate students from a public university in the United States. The final version of the vignette is provided in Appendix A.

3.2 | Participants

For the main administration of the experiment, we recruited a pre-screened pool of 200 individuals with work experience in sales using Amazon's Mechanical Turk (MTurk) (pre-screening question: "Please indicate how many years of work experience you have collected in each of the functions listed below: Finance, Accounting, IT, Procurement, Legal, Sales, Human Resources, Other (please specify)"). We adhered closely to recommended best practices in conducting our research through this platform (Mason & Suri, 2012). Rand (2012) conducted a study finding demographic responses provided by MTurk participants to be highly accurate, and Lee, Seo, and Siemsen (2018) successfully replicated numerous laboratory experiments using MTurk respondents. Studies by Downs, Holbrook, Sheng, and Cranor (2010) and Peer, Vosgerau, and Acquisti (2014) determined that data from this source was quite reasonable, surmising that Amazon's internal reputation systems keep quality levels high. Although Amazon prevents duplicate worker accounts, we also evaluated the data for duplicate IP addresses or GPS locations, and found none (Dennis, Goodson, & Pearson, 2018).

Twelve participants failed at least one of two direct query instruction checks (Abbey & Meloy, 2017) and were deleted from the sample. Instruction checks are shown in Appendix B. Of the remaining 188 responses, seven participants indicated less than 1 year of experience in a *professional sales role* and were deleted (demographics question: "How many years of work experience do you have in a professional sales role?"). Among the 181 usable responses, our research participants had an average age of 42.6 years and 21.2 years of overall work experience, with 8 years of professional experience in sales; 58% of the participants were female. Demographic data of the four research groups are displayed in Table 1.

3.3 | Measures

We included questions to assess our mediating variable of trust, and our ultimate dependent variable of information sharing willingness. The ability- and integrity-based trust items were adapted from Mayer and Davis (1999). The information sharing willingness construct was adapted from Eckerd and Sweeney (2018). A 7-point Likert-type scale was used for all items, ranging from 1 = "strongly disagree" to 7 = "strongly agree." All items are provided in Appendix C. Because studies have indicated potentially different moral judgments based on research participants' age (Deshpande, 1997; Razzaque & Hwee, 2002) and gender (Fleischman & Valentine, 2003; Okleshen & Hoyt, 1996), we included these items as control variables in our regression-based mediation and moderation analyses. We further included work experience as a control variable, which has been found to be a significant control variable in a relatively recent study on the negative events of supply disruptions (Polyviou et al., 2018).

TABLE 1 Demographic data of research participants per treatment group

	Inadvertent	Opportunistic
Dissimilarity	47 participants; Avg. age (yrs.) = 41.7 (*SD* = 12.1); 55.3% female	45 participants; Avg. age = 42.7 (*SD* = 13.0); 57.8% female
Similarity	46 participants; Avg. age = 42.4 (*SD* = 10.1); 60.9% female	43 participants; Avg. age = 43.8 (*SD* = 11.1); 58.1% female

3.4 | Experimental checks

We assessed the degree to which participants understood the vignettes to be realistic. Realism check questions used a 7-point Likert-type scale (1 = "strongly disagree" and 7 = "strongly agree"). The realism checks from the final experiment indicate that participants strongly perceived the scenarios as realistic (i.e., "The situation described was realistic", $\bar{x} = 6.14$, $SD = 0.808$; and "I had no difficulty imagining myself in the situation", $\bar{x} = 5.94$, $SD = 1.207$).

We also conducted manipulation checks to confirm that the manipulations worked as intended (see Appendix B). These questions also are based on a 7-point Likert-type scale (1 = "strongly disagree" and 7 = "strongly agree"). Univariate analyses of the manipulation checks show significant differences across all treatments, indicating that the treatments were indeed salient to the participants, that is, intentionality (inadvertent: $\bar{x} = 1.95$, opportunistic: $\bar{x} = 6.45$, $p = .000$), and operational similarity (dissimilarity: $\bar{x} = 1.63$, similarity: $\bar{x} = 6.21$, $p = .000$). For the statistical analyses of H1a, H1b, H1c, both intentionality and operational similarity were coded as binary variables, where intentionality = 0 represents inadvertent and operational similarity = 0 represents operationally dissimilar. For the analyses of H2a, H2b, and H3, we used the manipulation check responses for intentionality as our independent variable, allowing for separate mediation analyses of each intentionality group. We assessed the pre-treatment levels of information sharing willingness and both trust variables as a check to ensure that no differences between treatments emerged that we had not accounted for. These tests reveal no significant differences in the information sharing willingness levels across groups (intentionality $p = .943$, operational similarity $p = .458$, intentionality × operational similarity $p = .573$) and no significant differences in the pre-treatment trust levels across groups (integrity-based trust: intentionality $p = .890$, operational similarity $p = .798$, intentionality × operational similarity $p = .935$; ability-based trust: intentionality $p = .190$, operational similarity $p = .700$, intentionality × operational similarity $p = .888$).

4 | RESULTS

4.1 | Validity and reliability

Confirmatory factor analysis of the post-treatment data shows a reasonable overall fit of the model, consistent with recommended indices ($\chi^2 = 171.74$, d.f. = 84; χ^2/d.f. = 2.045; RMSEA = 0.076; CFI = 0.971; AGFI = 0.849) (Bentler & Bonett, 1980; Browne & Cudeck, 1992; Hu & Bentler, 1999; Shah & Goldstein, 2006). Construct validity was assessed via convergent and discriminant validity for the measured constructs of integrity-based trust, ability-based trust, and information sharing willingness. Convergent validity was determined by the average variance extracted (AVE), with all values being higher than the recommended minimum value of 0.5 (Bagozzi & Yi, 1988) (see Table 2). Discriminant validity does not appear to be a concern because the maximum shared variance (MSV) lies below the AVE and because the AVE square root is higher than the inter-construct correlations for each construct. Finally, the inter-construct correlations are all below the recommended maximum threshold of 0.85 (Brown, 2006; Hair, Black, Babin, & Anderson, 2010). Validity and reliability results are provided in Table 2; standard errors and standardized loadings are shown in Appendix C.

All composite reliability (CR) values exceed the recommended minimum threshold of 0.6 (Bagozzi & Yi, 1988). Finally, the Cronbach's alphas for integrity-based trust, ability-based trust, and information sharing willingness are 0.95, 0.90, and 0.97, respectively, thus exceeding the recommended minimum threshold of 0.7 for internal consistency (Robinson, Shaver, & Wrightsman, 1991).

4.2 | Hypothesis testing

We used a paired-samples *t*-test for the testing of H1a and H1b (see Table 3). When comparing the respective scores, information sharing willingness decreased significantly and by approximately 22.63% in the inadvertent treatment (t (92) = 10.117, $p = .000$; CI [1.077; 1.604]), providing support for H1a. In the opportunistic treatment, the information sharing willingness mean score decreased by approximately 56.08% (t (87) = 21.176, $p = .000$; CI [3.007; 3.630]), providing support for H1b.

In addition, we conducted an ANOVA on ex post information sharing willingness for the testing of H1c. In an experimental ANOVA approach, "(...) manipulated regressors are *plausibly exogenous*" (Ketokivi & McIntosh, 2017, p. 9), as the random allocation of participants to the treatment groups minimizes potential endogeneity problems.[2] The results reveal that the scores are significantly lower in the opportunistic treatment than in the inadvertent treatment (F [1, 179] = 108.486; $p = .000$) and as such, provide support for H1c. Figure 3 shows a graphical summary of the information sharing willingness mean scores across the four different groups before and after the information leakage.

TABLE 2 Validity and reliability results

	Composite reliability (CR)	Average variance extracted (AVE)	Maximum shared variance (MSV)	Ability-based trust	Integrity-based trust	Information sharing willingness
Ability-based trust	0.903	0.610	0.202	**0.781**		
Integrity-based trust	0.956	0.786	0.696	*0.389*	**0.887**	
Information sharing willingness	0.970	0.916	0.696	*0.449*	*0.834*	**0.957**

Notes: Values in bold display the AVE square roots, values in italics display the inter-construct correlations.

TABLE 3 Ex ante and ex post information sharing willingness (ISW)—paired samples statistics

Intentionality	Variable	Mean	n	*SD*	*SE*
Inadvertent	Ex ante ISW	5.925	93	0.692	0.072
	Ex post ISW	4.584	93	1.329	0.138
Opportunistic	Ex ante ISW	5.917	88	0.721	0.077
	Ex post ISW	2.599	88	1.230	0.131

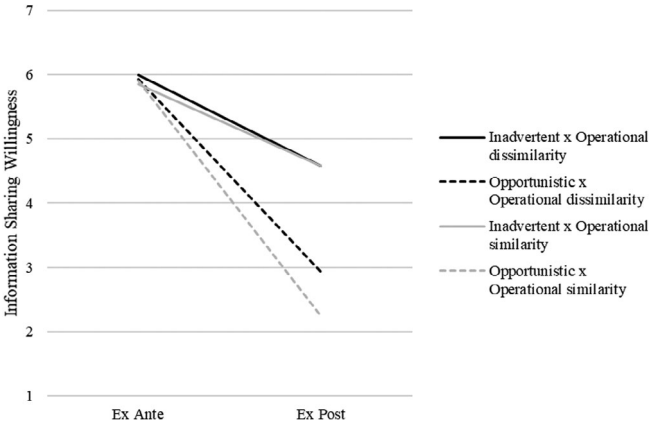

FIGURE 3 Information sharing willingness mean scores per treatment group

4.2.1 | Mediation analysis

We analyzed mediation and moderation (Subsection 4.2.2) effects with the post-treatment data separately for each type of intentionality (inadvertent vs. opportunistic), using model 4 for mediation (Hayes, 2013, pp. 125–130, 445) and model 7 for moderated mediation (Hayes, 2013, pp. 329–333, 447) of the PROCESS add-on of SPSS. These analyses were conducted via bias-corrected bootstrapping (bootstrapping sample of 5,000; bias-confidence interval of 95%), which is shown to have high statistical power (Taylor, MacKinnon, & Tein, 2008). We followed the analysis steps recommended by Rungtusanatham, Miller, and Boyer (2014) for mediation analysis via bootstrapping.

The indirect effect of intentionality on information sharing willingness through integrity-based trust does not include zero in its confidence interval for either type of intentionality (inadvertent: [−0.337; −0.015]; opportunistic: [−0.751; −0.230]), while the confidence interval for ability-trust includes zero in both types of intentionality (inadvertent: [−0.221; 0.067]; opportunistic: [−0.073; 0.019]) (see Tables 4 and 5). As such, the indirect effect through integrity-based trust is significant and mediation via integrity-based trust is established in both intentionality types. Because the direct effect of intentionality on information sharing willingness is insignificant in both intentionality types (inadvertent: $b = 0.023$, $t\ (86) = 0.346$, $p = .730$; opportunistic: $b = -0.189$, $t\ (81) = -1.044$, $p = .300$) (see Tables 6 and 7), the effect of integrity-based trust is an "indirect-only" mediation. With integrity-based trust as a mediator in both intentionality types and ability-trust being no mediator in either intentionality type, H2a is rejected and H2b is supported.

Figures 4 and 5 show graphical summaries of the mean scores for integrity- and ability-based trust across the four different groups before and after the information leakage.

4.2.2 | Moderated mediation analysis

Although ability-based trust is found to be a significant predictor of information sharing willingness in the case of an inadvertent leakage, no significant mediation is determined in either intentionality type, ruling out a potential moderated mediation. No significant effect is further observed when testing for moderated mediation of the integrity-based trust variable in either of the

TABLE 4 Inadvertent leakage

	Effect	*SE*	LLCI	ULCI
Total	−0.140	0.131	−0.467	0.045
Ex post integrity-based trust	−0.101	0.078	−0.337	−0.015
Ex post ability-based trust	−0.039	0.073	−0.221	0.067

Note: Regression results—indirect effects of intentionality on information sharing willingness.
Abbreviations: LLCI, lower limit confidence interval; ULCI, upper limit confidence interval.

TABLE 5 Opportunistic leakage

	Effect	*SE*	LLCI	ULCI
Total	−0.455	0.133	−0.757	−0.230
Ex post integrity-based trust	−0.452	0.132	−0.751	−0.230
Ex post ability-based trust	−0.004	0.021	−0.073	0.019

Note: Regression results—indirect effects of intentionality on information sharing willingness.
Abbreviations: LLCI, lower limit confidence interval; ULCI, upper limit confidence interval.

TABLE 6 Inadvertent leakage

	b	*SE*	*t*	*p*	LLCI	ULCI
Constant	−1.879	0.665	−2.824	0.006	−3.201	−0.556
Main effect						
Intentionality	0.023	0.066	0.346	0.730	−0.108	0.153
Mediating effects						
Ex post integrity-based trust	0.539	0.145	3.713	0.000	0.251	0.828
Ex post ability-based trust	0.639	0.138	4.623	0.000	0.364	0.913
Control variables						
Age	0.027	0.016	1.689	0.095	−0.005	0.059
Gender	−0.270	0.165	−1.640	0.105	−0.597	0.057
Work experience	−0.023	0.017	−1.422	0.159	−0.056	0.009

Note: Regression results on information sharing willingness with mediators. *Model summary:* $R = 0.831$, $R^2 = 0.691$, MSE = 0.584, $F = 32.069$, df1 = 6, df2 = 86, $p = .000$.
Abbreviations: LLCI, lower limit confidence interval; ULCI, upper limit confidence interval.

intentionality types (PROCESS model 7, Hayes, 2013, pp. 329–333, 447), as the index of moderated mediation includes zero in its confidence interval (inadvertent: [−0.233; 0.431]; opportunistic: [−0.573; 0.430])[3] (see Tables 8 and 9). Hence, no moderated mediation is prevalent for either trust dimension and no support is found for H3.

4.3 | Quantitative post hoc analysis

Although no moderation effect was supported for the relationship between intentionality and the trust variables based on operational similarity, ANOVA for each intentionality treatment provides a more nuanced understanding of the data (Table 10).

We find that the scores for information sharing willingness of the two groups, "Inadvertent × Operational similarity" and "Inadvertent × Operational dissimilarity", are not significantly different from each other ($p = .974$), while the scores of the two groups, "Opportunistic × Operational similarity" and "Opportunistic × Operational dissimilarity", are significantly different ($p = .008$). Thus, the information sharing willingness is lower when *VICTIM* and *OBSERVER* are operationally similar than when they are operationally dissimilar in the case of an opportunistic leakage, as further visualized in Figure 3. Although this form of testing does not substitute previous findings on the hypothesized moderation of the relationship between intentionality and trust, it complements them by suggesting that different levels of similarity have a direct influence on

TABLE 7 Opportunistic leakage

	b	*SE*	*t*	*p*	LLCI	ULCI
Constant	1.077	1.546	0.697	0.488	−2.000	4.153
Main effect						
Intentionality	−0.189	0.181	−1.044	0.300	−0.550	0.171
Mediating effects						
Ex post integrity-based trust	0.843	0.124	6.794	0.000	0.596	1.089
Ex post ability-based trust	0.063	0.103	0.619	0.538	−0.141	0.268
Control variables						
Age	0.009	0.019	0.488	0.627	−0.029	0.048
Gender	0.087	0.221	0.394	0.694	−0.352	0.526
Work experience	−0.014	0.020	−0.689	0.493	−0.053	0.026

Note: Regression results on information sharing willingness with mediators. *Model summary:* $R = 0.683$, $R^2 = 0.467$, MSE = 0.866, $F = 11.814$, df1 = 6, df2 = 81, $p = .000$.
Abbreviations: LLCI, lower limit confidence interval; ULCI, upper limit confidence interval.

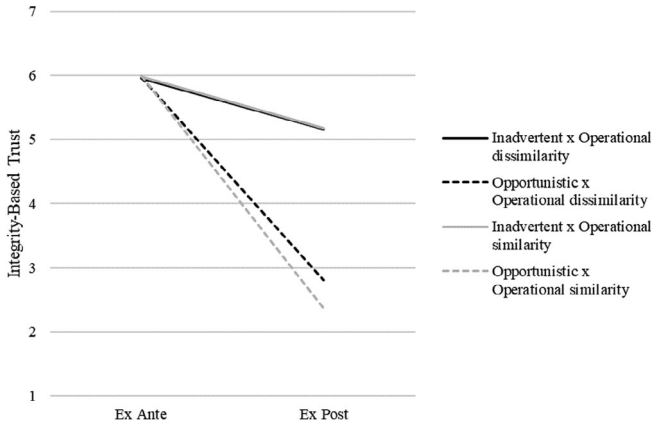

FIGURE 4 Integrity-based trust mean scores per treatment group

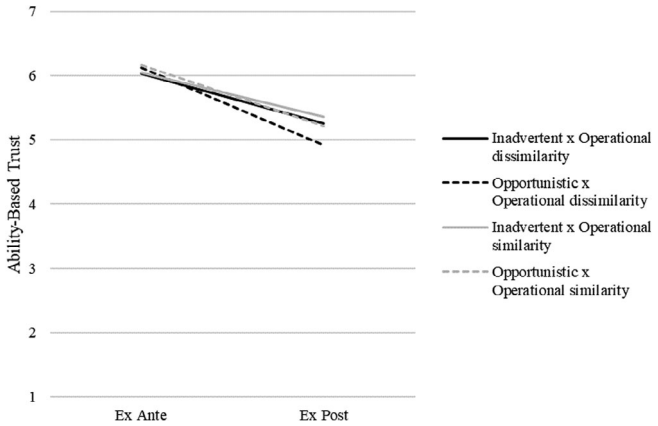

FIGURE 5 Ability-based trust mean scores per treatment group

information sharing willingness as the final outcome after an opportunistic information leakage, but not after an inadvertent one.

4.4 | Qualitative post hoc analysis

To help us better understand the relevance and meaning of our findings, especially for those that were counterintuitive to our expectations, we used a sequential explanatory strategy (Creswell & Plano Clark, 2018) and conducted several post-experimental interviews. This qualitative approach in addition to the previous quantitative analyses allows for between-method triangulation of our observations (Denzin, 2009). In particular, the interviews provide additional context and grounding for the discussion of our theoretical contributions, managerial implications, and opportunities for future research. With the interview questions (see Appendix D), we sought to collect practical evidence regarding inter-organizational information leakages and their effects on the quality of business relationships, as well as on managers′ decisions afterwards.

For this analysis, we interviewed eight experienced sales managers (ranging from 12 to 36 years of work experience), strengthening the external validity/realism of our study (McGrath, 1982). These managers were employed in large-sized organizations in North America, Europe, and Asia. Industries represented included chemicals, construction & mining, consumer goods, and medical technologies (see Appendix E). Each interview was conducted via telephone and lasted 25–53 min ($\bar{x} = 40$ min). In the subsections below, we followed the recommended procedure of including both power quotes and proof quotes to effectively illustrate our qualitative findings (Pratt, 2008, 2009).

4.4.1 | Information leakage spillovers

Our first objective with the interviews was to assess once more the categorization of inadvertent and opportunistic

TABLE 8 Inadvertent leakage

	Index	*SE*	LLCI	ULCI
Ex post integrity-based trust	0.046	0.154	−0.233	0.431
Ex post ability-based trust	0.021	0.158	−0.287	0.346

Note: Index of moderated mediation.
Abbreviations: LLCI, lower limit confidence interval; ULCI, upper limit confidence interval.

TABLE 9 Opportunistic leakage

	Index	*SE*	LLCI	ULCI
Ex post integrity-based trust	−0.066	0.252	−0.573	0.430
Ex post ability-based trust	0.016	0.062	−0.042	0.247

Note: Index of moderated mediation.
Abbreviations: LLCI, lower limit confidence interval; ULCI, upper limit confidence interval.

TABLE 10 Ex post information sharing willingness—ANOVA (operational similarity vs. dissimilarity)

Intentionality	Source	Type III sum of squares	df	Mean square	*F*	Sig.
Inadvertent	Corrected model	0.002	1	0.002	0.001	0.974
	Intercept	1954.143	1	1954.143	1,093.725	0.000
	Operational similarity	0.002	1	0.002	0.001	0.974
	Error	162.588	91	1.787	–	–
	Total	2,117.000	93	–	–	–
	Corrected total	162.590	92	–	–	–
Opportunistic	Corrected model	10.326	1	10.326	7.323	0.008
	Intercept	590.326	1	590.326	418.653	0.000
	Operational similarity	10.326	1	10.326	7.323	0.008
	Error	121.265	86	1.410	–	–
	Total	725.778	88	–	–	–
	Corrected total	131.591	87	–	–	–

information leakages, and to do so by determining whether observations of each of these types of leakages commonly took place and could be identified at a network level. Our interviewees provided us with a deeper understanding of leakages happening within their respective industries and revealed that leakages could indeed be attributed to different causes.

All except two interviewees were able to report at least one information leakage on a network level caused by a customer in the past, either of inadvertent nature or opportunistically motivated (for proof quotes, see Appendix F). Further, interviewees reported incidents that they learned about through trusted sources (similar to the lens used in the experiment of this study), as well as incidents where they received leaked information themselves. These insights both support that scenarios such as the ones from the experiment indeed are common in practice, and complement our findings by pointing us to information leakages where an *OBSERVER* becomes the actual *RECEIVER* of information. Interestingly, although most *RECEIVER*s benefited from gaining access to the leaked information through the *OFFENDER* and one might argue for a resulting positive impact on the relationship between *RECEIVER* and *OFFENDER*, reactions in terms of trust and information sharing willingness did not seem to differ compared to those incidents where interviewees merely observed a leakage.

The interviews overall made it clear that the intentionality attribution for the event made a tremendous difference in the way it was perceived and the response it engendered. One noteworthy observation was that assumed repeatability played a role in the interviewees′ responses: Most recognized that inadvertent leakages were likely more isolated and less frequently repeated incidents, as for example reflected in a statement from Supplier 4:

> "We are all human beings. We can all make mistakes. So as long as it is not a repeating

> mistake, I think I would be open to giving my distributor another chance." *(Supplier 4)*

However, caution increased when the leakage was opportunistic, seemingly due to rising concerns of a similar fate in the future:

> "...if we find out a retailer is using stolen information in the marketplace or information that shouldn't be shared in the marketplace in order to drive their own business, it does lead to us to be more wary in doing deals with them. Because if they would take information from somebody else, it increases the potential odds that they would share our own information with someone else as well." *(Supplier 5)*

The aspect of repeatability posits a relevant notion, as it relates to attribution theory's stability dimension that was rationalized to be similar across both intentionality types. Although one might claim that systematic carelessness of the buyer (despite the leakage being inadvertent) could be the cause of even more leakages in the future than possibly only one opportunistically motivated leakage, the interviewees seemed to regard the opportunistic leakage as more representative for the future. This data suggests a potential interplay between the stability and intentionality dimensions of attribution; a phenomenon which will benefit from more in-depth studies in this area in the future.

4.4.2 | The role of trust in response to a leakage

Trust played a critical role in the sense-making processes following an information leakage, and our interviews helped us better understand the mechanisms at play. The qualitative data support a clear spillover effect, as trust towards the *OFFENDER* decreased although none of the interviewees were the actual *VICTIM* in any of the reported leakages. Interviewees reported both ability-based and integrity-based trust to be negatively affected after an information leakage. The interviews indicate that ability-based trust was clearly perceived an issue in inadvertent leakages, and integrity-based trust was paramount in opportunistic leakages. However, several interviewees also reported decreasing levels of ability-trust after an opportunistic leakage and reduced integrity-trust after an inadvertent leakage.

Indeed, against our hypothesis that ability-based trust would mediate the relationship between an inadvertent leakage and the *OBSERVER's* willingness to share information with the *OFFENDER*, our experiment revealed integrity-based trust to be the significant mediator and not ability-based trust. This may be due to *OBSERVERs'* interpretations that inadvertent leakages might not be random accidents, but rather a reflection of lacking integrity as a more fundamental cause, because *OFFENDERs* would require integrity to establish data security in the first place. Supplier 6 indicated this effect with the following statement:

> "...the customer did not have appropriate systems in place to prevent that accidental release and therefore, they don't have systems so they are not really thinking about that integrity part." *(Supplier 6)*

The complementary findings from our interviews indicate that although the quantitative analyses determined only integrity-trust to ultimately have a *significant mediating effect*, both trust levels may decrease to *some extent* after either leakage type (for proof quotes, see Appendix F). This suggests a potential collateral damage effect in trust, as can also be observed in the decreasing trust levels from before to after any information leakage in the plots of the quantitative analysis (Figures 4 and 5).

The overall effect on trust clearly differed between opportunistic and inadvertent leakages; interviewees experiencing opportunistic leakages reacted in a much more guarded manner. Supplier 5 even noted the dissemination of false information as a means of protection against opportunistic leakages:

> "They will send out a smoke signal or they'll basically send out fake ads to try to see and if they can figure out who or where the information is being leaked from. I've seen that happen; it gets to a point where the lack of integrity forces people to increase their resources and labor in order to protect their information in the market by basically putting two plans out there....It gets to the point where you get burned enough times, people will change their behavior patterns." *(Supplier 5)*

4.4.3 | The role of similarity in information leakages

The interviewees had varying opinions about the effects that operational similarity between the victim organization and their own had on reactions to information leakages. The comments of Supplier 4 reflect our experiment findings on operational similarity: The first concern is the attribution for the transgression, and not operational similarity:

> "I'll be concerned about the action that the distributer has taken vs. whether the victim supplier is similar to us or not. I don't think that really matters. It's more in principle what the distributer has shared is not correct." *(Supplier 4)*

Although the overall finding was that operational similarity showed no significant moderating effect on trust, Supplier 5 expressed that the visibility/salience of the event might well be increased with higher similarity between *OBSERVER* and *VICTIM*:

> "There is always going to be more emotions and closeness proximity....If something is closer to you, you're going to take more notice of it. Because it's easier to potentially see him—you know, that incident replicating to you." *(Supplier 5)*

5 | CONTRIBUTIONS, LIMITATIONS, AND FUTURE RESEARCH

5.1 | Theoretical contributions

Although information leakages are a primary concern in today's business environment, they remain vastly underinvestigated in the OSCM literature (Massimino et al., 2018). Moreover, despite a breadth of research focusing on dyadic buyer–supplier relationships, an increasing number of scholars have suggested that we need to expand our research frames to consider supply chain networks (Choi & Kim, 2008; Mena, Humphries, & Choi, 2013). Existing research on information sharing has largely examined networks in which one supplier faces multiple buyers (see, for example, Jain & Sohoni, 2015; Kong et al., 2013; Shamir, 2017), while the present study contributes to the relatively scant research body on information sharing in networks of one buyer and multiple suppliers (see, for example, Shang, Ha, & Tong, 2015). In following with these recommendations, we argue that information leakages can have a meaningful effect on the wider supply network.

Our work on the spillover effect provides a strong rationale for differentiating between information leakage attributions in future research. Prior research has tended to overlook issues related to how information leakages arise (Massimino et al., 2018); our work fills the gap and shows support for a lessened effect from inadvertent leakages—one that might be remediable with concerted efforts of the offending organization. Our work also complements other recent research that evaluates the effects of unintentional supplier errors (Chen, Rungtusanatham, & Goldstein, 2019) and that proposes stark differences in how inadvertent and intentional supply chain events might be handled (DuHadway et al., 2019; Speier et al., 2011).

In addition, we posited the mediating role of trust on the relationship between information leakage attribution and willingness to share information. We extended the concept of hierarchically restrictive schema to suggest that ability-based trust would be an important factor in responding to inadvertent leakages, that integrity-based trust would play a key role following opportunistic leakages, and that the latter effect would be stronger. The mediating role of integrity-trust was supported by our findings, demonstrating that integrity-based trust was not confined to mediating only opportunistic leakages, as hypothesized, but that it also mediated the relationship involving inadvertent leakages. This finding was unexpected, especially considering that the experiment described the offending buyer organization as one that had never been known to act "opportunistically or deceitfully toward your organization or any other organization in the industry" and as one that was "just and understanding toward other organizations." Hence, the *OFFENDER* was pictured as an organization of high integrity, as supported by the initial integrity-based trust mean value of 5.977 reported by participants prior to the information leakage. The scenario text in the inadvertent treatment made very clear that the *OFFENDER's* act of sharing the *VICTIM's* confidential information was unintentional; manipulation checks strongly supported clarity of the attribution's unintentionality. Nevertheless, participants significantly decreased their integrity-based trust in the *OFFENDER*, suggesting a collateral damage effect of inadvertent leakages on perceived levels of integrity.

As discussed in Subsection 4.4.2, the interview data indicates that both trust dimensions, integrity- and ability-based trust, may decrease to some extent in both leakage types, inadvertent and opportunistic. For instance, several suppliers observed that opportunistic leakages led them to believe the offender was incompetent, with one stating that "it undermines what I think of his knowledge and technical skills" *(Supplier 3)*. Similarly, although only integrity-based trust was shown to be a significant mediator for the relationship between any leakage and information sharing willingness, the quantitative data also indicates a slight decrease of ability-based trust in both leakage types. Revelation of these collateral effects was rather unexpected in accordance with developments surrounding hierarchically restrictive schema (Reeder & Brewer, 1979), yet they were corroborated by

our interviewees. We recognize that most of the literature evaluating the applicability of hierarchically restrictive schema as it pertains to integrity- and competence-based trust has been conducted at the intra-organizational level (Dirks, Kim, Ferrin, & Cooper, 2011; Kim, Dirks, Cooper, & Ferrin, 2006). However, arguments have meaningfully distinguished the intra-organizational level from the inter-organizational level (Lumineau, Eckerd, & Handley, 2015). Likewise, our work extends and challenges the direct applicability of previous findings for the intra-organizational level to an inter-organizational network.

Finally, our findings indicate that although no overall moderation effect was observed, operational similarity between the *VICTIM* and the *OBSERVER* seems to influence the *OBSERVER's* learning effect after an opportunistic information leakage, but not after an inadvertent one. This finding could perhaps be explained by the inherent direction of the opportunistic leakage: The *OFFENDER* was aware of the fact that the opportunistic leakage would harm the *VICTIM* but still executed it, while the inadvertent leakage might be perceived as being more of a mistake that could happen to anyone, as expressed by Supplier 4 in the interviews (see Subsection 4.4.1). This finding lends support to the group-identity mechanism (e.g., Menges & Kilduff, 2015; Smith et al., 2007; Urda & Loch, 2013), in that an *OBSERVER* might perceive random accidents as less of an attack on their "in-group" of operationally similar suppliers, compared to opportunistic events.

5.2 | Managerial implications

We theorized that information leakages between a buyer and supplier would cause spillover effects on observers in the wider supply network. Indeed, we empirically found these effects to be the case. Observational learning plays an important role in the future relationship an *OBSERVER* has with an *OFFENDER*, in that it leads to significant degradations in information sharing willingness, regardless of the rationale for the leakage. This response is an important and—as our interviewees pointed out—necessary protection mechanism; the harm caused by the leakage of certain types of information is too substantial to take the risk. Studies have shown that information leakages can lead to losses of competitive advantage for any type of organization when that information is being shared with current or potential future competitors (Hoecht & Trott, 2006; Kurtuluş & Toktay, 2009). In fact, some companies rely so heavily on the confidentiality of certain information—such as Coca-Cola regarding the trade secret of its original beverage recipe—that the distribution of it could threaten the organization's very survival (Hettinger, 1989). Nevertheless, avoidance learning could potentially act as a double-edged sword: Apart from the potential protection arising from the avoidance of information leakage events, the excessive avoidance of information sharing could cause the *OBSERVER* to miss out on valuable information sharing benefits in the future. Managers therefore face trade-offs when making decisions on information sharing (Cezar, Cavusoglu, & Raghunathan, 2014, 2017). Given the high sensitivity of the topic of information sharing for practice, we derive implications for both *OBSERVERs* and *OFFENDERs*.

We recommend to *OBSERVERs* that when observing an information leakage, they need to understand *why* the leakage occurred—that is, whether it happened inadvertently or opportunistically. By understanding the rationale, *OBSERVERs* might be in a better position to assess their potentially biased trust judgments after the event. This understanding might be particularly relevant in the case of inadvertent events because our findings revealed that an inadvertently caused leakage led *OBSERVERs* to question an *OFFENDER's* fairness, honesty, values, or sense of justice, even though the *OFFENDER's* integrity was by all accounts unscathed. The risk of collateral damage to integrity-based trust levels is that it can unnecessarily impede information sharing. This effect can be particularly damaging in light of the reciprocal nature of information sharing; the supply chain risks dilution of its interdependent nature (Lejeune & Yakova, 2005). Consequently, discontinuing information sharing following a seemingly unimportant slip might lead to a vicious cycle of considerably less collaboration and value in the overall network of relationships. Further studies could evaluate the potential for information leakages to lead to such a downward spiral.

To illustrate this effect, all parties might benefit from recognizing how to further proactively address inadvertent information leakages. Given the clear negative effect on integrity-based trust and indications that ability-based trust may be affected negatively as well based on our interview data (see Appendix F) and on decreases in ability-based trust in our experiment (see Figure 5) despite them being statistically insignificant, a meaningful and swift remediation effort might help allay *OBSERVERs'* concerns when a more practical systems-based resolution could constitute a more reasonable response. Supplier 5 best illustrated this potential in the following response:

> "I've dealt with buyers who accidentally copied me instead of a competitor on an email.... How do you make sure that you and your team take the proper steps to [safeguard] information that we send to them...? [If] it's

> because of their systems and structure, meaning that we realize that their processes are too open or they have multiple people touching the information and they don't have true safeguards, then that would be an even deeper discussion, because that's something that's still within their control. They just haven't put up the firewalls between different departments or different functions to guard the information....[We] need proof, that your IT team or whoever, legal team has put the firewall in place to protect the information if we are going to continue the partnership at this level." *(Supplier 5)*

The following statement from another supplier further suggests that confidentiality agreements as prevention tools for information leakages do not suffice, supporting the notion that more proactive actions from *OFFENDERs* might be necessary:

> "Of course, we try to do as much as we can with confidentiality agreements, but can we always prevent that things are leaking into the market? The answer would be no." *(Supplier 1)*

OFFENDERs can volunteer to undertake these proactive efforts as a show of good faith, or *OBSERVERs* still desiring to reap the benefits of information sharing with an *OFFENDER* while allaying concerns of repeatability can ask the *OFFENDER* to implement these or similar actions. Moreover, we recommend to *OFFENDERs* that after they become aware of an information leakage, they must assume responsibility and not engage in blame shifting (Park, Park, & Ramanujam, 2018). To regain trust, buyers that cause a leakage can also initiate a fresh start in meetings with their suppliers immediately following the event (Kaufmann, Esslinger, & Carter, 2018; Rizvi & Bobocel, 2016). Ongoing measures might include reflection modules during trainings and meetings, similar to those in which health and safety awareness is raised. These practices can become a regular occurrence in cross-company projects and meetings, with the goal of building a shared security mindset as a core element of a resilient, high-reliability relationship (Fraher, Branicki, & Grint, 2017; Weick & Roberts, 1993).

5.3 | Limitations and future research

We acknowledge several limitations of the present study, and related opportunities to expand on this line of research. First, although we highlighted in the instructions for the experiment that participants could assume the scenario information to be accurate, we did not provide detailed information on how the observer learned about the leakage, except to state that the news came from a highly reliable source that could be trusted, and participants could assume the information was true. The purpose of this design decision was to reduce complexity; our two pilot studies had contained more detailed information but were viewed by the participants as too complex. However, the source of the information leakage might be an important variable to consider (e.g., whether the *OBSERVER* learns about the event via news reports or from direct and proactive confessions from the *OFFENDER*).

Second, although we took several actions in the design to control for (i.e., exclude) the possibility that the *OBSERVER* benefited from an information leakage occurring between the *OFFENDER* and *VICTIM*, it is conceivable that through a longer chain of events, the *OBSERVER* might ultimately experience some benefits. The vignette made it clear that *OBSERVER* and *VICTIM* had no existing relationship with each other, including no competition, and that neither of the two firms were intending to enter each other's businesses. Nevertheless, in situations where a *VICTIM* is affected by a leakage to an extent that it is required to reduce its operations or proactively exits the business relationship with the *OFFENDER*, under specific circumstances the *OFFENDER* might shift its business and expand cooperation with the *OBSERVER*.

Third, our empirical approach uses scenario-based experiments grounded in social psychology to evaluate our research question. Although this approach itself is not a limitation, we are mindful of the trade-off between internal and external validity that such design decisions imply. We further enhance external validity of the findings through the interviews we conducted. However, future research might supplement the use of such analytical approaches (already commonly implemented in information sharing research in OSCM) with economics-based experiments. This complementary approach to the problem allows for triangulation of multiple methods across a broad program of research and will prove most beneficial to a comprehensive understanding of the information sharing problem (Boyer & Swink, 2008).

Fruitful paths for future research are numerous, and we summarize additional opportunities in Data S1. For example, similar to previous research finding a cyclical effect of relationship strength and performance over time (Autry & Golicic, 2010), the history of information sharing between the buyer and supplier could be an important factor to examine further in future research. Insights

from system dynamics (Forrester, 1968) illustrate that learning is in large part a function of exposure to a system over time (Argote, Beckman, & Epple, 1990). In accordance with system dynamics thinking, a buyer–supplier interaction evolves over time and provides valuable knowledge pertinent to future decision making, including the quality of information sharing efforts (Bendoly, 2014). This is also consistent with the literature expounding on the "shadow of the past", wherein the learning that occurs over time is anticipated to increase expectation of relationship continuity, which in turn drives behaviors differently than would be expected in situations with no prior history (Poppo, Zhou, & Ryu, 2008). Thus, while our research using an experiment controlled for prior history, it appears highly beneficial to examine how learning via a history of interactions might complement these results.

Another particularly intriguing area for future research involves a more thorough investigation into the effects of power and dependence in these relationships (see, for example, Benton & Maloni, 2005; Dong, Liu, Yu, & Zheng, 2015). In our research, we controlled for symmetries in the power and dependence of the entities, but this very often may not be the case in practice. For example, take the situation wherein a supplier is locked-in to their relationship with a buyer (Narasimhan, Nair, Griffith, Arlbjørn, & Bendoly, 2009); the supplier may not be afforded the option in such a situation to avoid sharing information with their buyer. Moreover, as the interdependence between a buyer and supplier increases, we conjecture this may change the dynamics of information sharing in the relationship. Research at the individual level has shown that different types of interdependence (i.e., outcome interdependence vs. task interdependence) cause different outcomes (Bendoly, Croson, Goncalves, & Schultz, 2010). For instance, Schoenherr, Bendoly, Bachrach, and Hood (2017) investigated reciprocal effects in task interdependent project teams, and while their results were somewhat mixed when considering positive versus negative inequities, as they note the context of the study matters immensely. Individuals making decisions on behalf of the entire organization may be differently bounded in their degrees of freedom in reconstituting equities.

This also points strongly to the influence of the individual in decisions involving information sharing. Our work focused on individuals as the ambassador of the organization, and as such did not undertake a full-scale examination of individual-level factors that could impact these decisions. Future research could parse out these individual level phenomena, and their impact on information sharing willingness. For example, Loch and Wu (2008) demonstrated the effect that a cooperative relationship exhibited on economic decisions in a two-player market experiment. While social capital has been evaluated previously as an organizational level construct (Lawson, Tyler, & Cousins, 2008; Villena, Revilla, & Choi, 2011), individual level business relationships are common occurrences, as well (Price & Arnould, 1999; Swan, Goodwin, Mayo, & Richardson, 2001). Another factor that is likely to prove relevant in these relationships is psychological safety. Psychological safety in our context would refer to boundary spanners feeling like they could make decisions about information sharing without risk of negative occupational consequences (Loch, 2017), and learning has been shown more effective in situations described as psychologically safe (Edmondson, 1999). Research in OSCM has demonstrated the importance of psychological safety to information sharing in an intra-organizational context (Siemsen, Roth, Balasubramanian, & Anand, 2009); particularly given our context involving sensitive information leakages, we would expect psychological safety to play a key role in this environment, as well.

In addition, further explorations of the effects of receiving leaked information on the relationship between the *OFFENDER* and the actual *RECEIVER* could be interesting. One supplier suggested, when referring to opportunistic information leakages, that obtaining sensitive information from the *OFFENDER* might in fact bring both parties closer together on an interpersonal level:

> "He is almost treating us more like part of his own company than as an external partner by sharing that information. And in part that is what they want to do, they want to establish that relationship by sharing something that they know is maybe not really to be shared to bring us closer." *(Supplier 6)*

A sense of obligation might even arise to return the favor of sharing sensitive information:

> "Maybe in the past this person helped you and now I have information from somewhere else which may be confidential but I want to share it with you." *(Supplier 4)*

However, fear of a similar fate seems to counteract any potential relationship strengthening aspects between *OFFENDER* and *RECEIVER* that leaking sensitive information might have, as pointed out by Supplier 6 and Supplier 7:

> "If the customer is willing to share that information with us, it means he is also willing to

> do the same with our competitor." *(Supplier 6)*
> "When a customer shares information with us about our competitors, I can imagine that the same thing can happen with a competitor of me, so that my customer may share some information... to my competitors." *(Supplier 7)*

Based on these qualitative data, empirical investigations into how the different mechanisms relate to each other would provide a deeper understanding of the manifold consequences of information leakages.

Acknowledgment

We are grateful for the valuable comments from Mikaella Polyviou on an early version of the manuscript, and for the constructive comments of the editorial team throughout the entire review process.

ORCID

Leopold Ried https://orcid.org/0000-0002-8263-1214
Stephanie Eckerd https://orcid.org/0000-0002-9996-4752

ENDNOTES

[1] We use the terms "inadvertent" and "opportunistic" in this research; however, we acknowledge that several different terms are used synonymously with these two. Other terms used to indicate "inadvertent" include "accidental" and "unintentional," whereas "opportunistic" has also been termed "purposeful," "forcible," "deliberate," and "intentional" in various literatures (Anand & Goyal, 2009; Hoecht & Trott, 2006; Kong, Rajagopalan, & Zhang, 2017; Ritala, Olander, Michailova, & Husted, 2015; Tan, Wong, & Chung, 2016).

[2] The robustness of ANOVA is bolstered, as (a) the data was randomly and independently sampled, meeting the assumption of independence; (b) the Shapiro–Wilk test reveals that residuals of information sharing willingness are normally distributed ($p = .128$); and (c) the Levene's test shows that the assumption of homogeneity of variances is met ($p = .352$).

[3] The analysis was conducted with operational similarity as a dichotomous variable according to the actual group allocation (0 = operationally dissimilar, 1 = operationally similar). Similar results were obtained when conducting the analysis with the manipulation check data for operational similarity.

REFERENCES

Abbey, J. D., & Meloy, M. G. (2017). Attention by design: Using attention checks to detect inattentive respondents and improve data quality. *Journal of Operations Management*, *53-56*(1), 63–70.

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, *42*, 27–39.

Anand, K. S., & Goyal, M. (2009). Strategic information management under leakage in a supply chain. *Management Science*, *55*(3), 438–452.

Argote, L., Beckman, D. L., & Epple, D. (1990). The persistence and transfer of learning in industrial settings. *Management Science*, *36*(2), 140–154.

Autry, C. W., & Golicic, S. L. (2010). Evaluating buyer–supplier relationship–performance spirals: A longitudinal study. *Journal of Operations Management*, *28*(2), 87–100.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94.

Bandura, A. (1971). Vicarious and self-reinforcement processes. In R. Glaser (Ed.), *The nature of reinforcement* (pp. 228–278). Merrill, New York: Academic Press.

Baum, J. A. C., Li, S. X., & Usher, J. M. (2000). Making the next move: How experiential and vicarious learning shape the locations of chains' acquisitions. *Administrative Science Quarterly*, *45*(4), 766–801.

Bendoly, E. (2014). System dynamics understanding in projects: Information sharing, psychological safety, and performance effects. *Production and Operations Management*, *23*(8), 1352–1369.

Bendoly, E., Croson, R., Goncalves, P., & Schultz, K. (2010). Bodies of knowledge for research in behavioral operations. *Production and Operations Management*, *19*(4), 434–452.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, *88*(3), 588–606.

Benton, W. C., & Maloni, M. (2005). The influence of power driven buyer/seller relationships on supply chain satisfaction. *Journal of Operations Management*, *23*(1), 1–22.

Borgatti, S. P., & Cross, R. (2003). A relational view of information seeking and learning in social networks. *Management Science*, *49*(4), 432–445.

Boyer, K. K., & Swink, M. L. (2008). Empirical elephants – Why multiple methods are essential to quality research in operations and supply chain management. *Journal of Operations Management*, *26*(3), 338–344.

Brass, D. J., Butterfield, K. D., & Skaggs, B. C. (1998). Relationships and unethical behavior: A social network perspective. *Academy of Management Review*, *23*(1), 14–31.

Brown, T. (2006). CFA with equality constraints, multiple groups, and mean structures. In D. A. Kennedy (Ed.), *Confirmatory factor analysis for applied research* (pp. 236–319). New York, NY: Guilford Press.

Browne, M. W., & Cudeck, R. (1992). Alternative ways of assessing model fit. *Sociological Methods & Research*, *21*(2), 230–258.

Burke, C. J., Tobler, P. N., Baddeley, M., & Schultz, W. (2010). Neural mechanisms of observational learning. *Proceedings of the National Academy of Sciences of the United States of America*, *107*(32), 14431–14436.

Cai, S., Jun, M., & Yang, Z. (2010). Implementing supply chain information integration in China: The role of institutional forces and trust. *Journal of Operations Management*, *28*(3), 257–268.

Cao, M., & Zhang, Q. (2011). Supply chain collaboration: Impact on collaborative advantage and firm performance. *Journal of Operations Management*, *29*(3), 163–180.

Carr, A. S., & Pearson, J. N. (1999). Strategically managed buyer–supplier relationships and performance outcomes. *Journal of Operations Management*, *17*(5), 497–519.

Carter, C. R., Kosmol, T., & Kaufmann, L. (2016). Toward a supply chain practice view. *Journal of Supply Chain Management*, *53*(1), 114–122.

Carter, J. R., & Miller, J. G. (1989). The impact of alternative vendor/buyer communication structures on the quality of purchased materials. *Decision Sciences*, *20*(4), 759–776.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2014). Outsourcing information security: Contracting issues and security implications. *Management Science*, *60*(3), 638–657.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2017). Sourcing information security operations: The role of risk interdependency and competitive externality in outsourcing decisions. *Production and Operations Management*, *26*(5), 860–879.

Chen, Y. S., Rungtusanatham, M. J., & Goldstein, S. M. (2019). Historical supplier performance and strategic relationship dissolution: Unintentional but serious supplier error as moderator. *Decision Sciences*, *50*(6), 1224–1258.

Choi, T. Y., & Kim, Y. (2008). Structural embeddedness and supplier management: A network perspective. *Journal of Supply Chain Management*, *44*(4), 5–13.

Choi, T. Y., & Wu, Z. (2009). Triads in supply networks: Theorizing buyer–supplier–supplier relationships. *Journal of Supply Chain Management*, *45*(1), 8–25.

Connelly, B. L., Crook, T. R., Combs, J. G., Ketchen, D. J., & Aguinis, H. (2018). Competence- and integrity-based trust in interorganizational relationships: Which matters more? *Journal of Management*, *44*(3), 919–945.

Corsten, D., Gruen, T., & Peyinghaus, M. (2011). The effects of supplier-to-buyer identification on operational performance – An empirical investigation of inter-organizational identification in automotive relationships. *Journal of Operations Management*, *29*(6), 549–560.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage.

Delerue, H., & Lejeune, A. (2010). Job mobility restriction mechanisms and appropriability in organizations: The mediating role of secrecy and lead time. *Technovation*, *30*(5–6), 359–366.

Dennis, S. A., Goodson, B. M., & Pearson, C. (2018). MTurk workers' use of low-cost "virtual private servers" to circumvent screening methods: A research note (SSRN scholarly paper no. ID 3233954). Retrieved from Social Science Research Network website: https://papers.ssrn.com/abstract, 3233954.

Denzin, N. K. (2009). *The research act: A theoretical introduction to sociological methods* (3rd ed.). Englewood Cliffs, NJ: Prentice Hall.

Deshpande, S. P. (1997). Managers' perception of proper ethical conduct: The effect of sex, age, and level of education. *Journal of Business Ethics*, *16*(1), 79–85.

Devaraj, S., Vaidyanathan, G., & Mishra, A. N. (2012). Effect of purchase volume flexibility and purchase mix flexibility on e-procurement performance: An analysis of two perspectives. *Journal of Operations Management*, *30*(7–8), 509–520.

Dirks, K. T., Kim, P. H., Ferrin, D. L., & Cooper, C. D. (2011). Understanding the effects of substantive responses on trust following a transgression. *Organizational Behavior and Human Decision Processes*, *114*(2), 87–103.

Dong, M. C., Liu, Z., Yu, Y., & Zheng, J. H. (2015). Opportunism in distribution networks: The role of network embeddedness and dependence. *Production and Operations Management*, *24*(10), 1657–1670.

Downs, J. S., Holbrook, M. B., Sheng, S., & Cranor, L. F. (2010). Are your participants gaming the system? Screening Mechanical Turk workeers. In: Proceedings of the SIGCHI conference on human factors in computing systems, ACM, New York, pp. 2399–2402.

DuHadway, S., Carnovale, S., & Hazen, B. (2019). Understanding risk management for intentional supply chain disruptions: Risk detection, risk mitigation, and risk recovery. *Annals of Operations Research*, *283*(1), 179–198.

Ebrahim-Khanjari, N., Hopp, W., & Iravani, S. M. (2012). Trust and information sharing in supply chains. *Production and Operations Management*, *21*(3), 444–464.

Eckerd, S., Hill, J., Boyer, K. K., Donohue, K., & Ward, P. T. (2013). The relative impact of attribute, severity, and timing of psychological contract breach on behavioral and attitudinal outcomes. *Journal of Operations Management*, *31*(7–8), 567–578.

Eckerd, S., & Sweeney, K. (2018). The role of dependence and information sharing on governance decisions regarding conflict. *The International Journal of Logistics Management*, *29*(1), 409–434.

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly*, *44*(2), 350–383.

Fiske, S. T., & Taylor, S. E. (1991). *Social cognition* (2nd ed.). New York: McGraw-Hill.

Fleischman, G., & Valentine, S. (2003). Professionals' tax liability assessments and ethical evaluations in an equitable relief innocent spouse case. *Journal of Business Ethics*, *42*(1), 27–44.

Flynn, B. B., Koufteros, X., & Lu, G. (2016). On theory in supply chain uncertainty and its implications for supply chain integration. *Journal of Supply Chain Management*, *52*(3), 3–27.

Forrester, J. W. (1968). *Principles of systems*. Cambridge, MA: MIT Press.

Fraher, A. L., Branicki, L. J., & Grint, K. (2017). Mindfulness in action: Discovering how U.S. navy seals build capacity for mindfulness in high-reliability organizations (HROs). *Academy of Management Discoveries*, *3*(3), 239–261.

Giunipero, L. C. (1990). Motivating and monitoring JIT supplier performance. *Journal of Purchasing & Materials Management*, *26*(3), 19–24.

Guglielmo, S., & Malle, B. F. (2010). Can unintended side effects be intentional? Resolving a controversy over intentionality and morality. *Personality & Social Psychology Bulletin*, *36*(12), 1635–1647.

Gulati, R. (1995). Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances. *Academy of Management Journal*, *38*(1), 85–112.

Gulati, R., & Sytch, M. (2008). Does familiarity breed trust? Revisiting the antecedents of trust. *Managerial and Decision Economics*, *29*(2–3), 165–190.

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Handley, S. M., & Benton, W. C., Jr. (2012). The influence of exchange hazards and power on opportunism in outsourcing

relationships. *Journal of Operations Management*, *30*(1–2), 55–68.

Handley, S. M., de Jong, J., & Benton, W. C., Jr. (2019). How service provider dependence perceptions moderate the power–opportunism relationship with professional services. *Production and Operations Management*, *28*(7), 1692–1715.

Hartmann, J., & Moeller, S. (2014). Chain liability in multitier supply chains? Responsibility attributions for unsustainable supplier behavior. *Journal of Operations Management*, *32*(5), 281–294.

Harvey, P., Madison, K., Martinko, M., Crook, T. R., & Crook, T. A. (2014). Attribution theory in the organizational sciences: The road traveled and the path ahead. *Academy of Management Perspectives*, *28*(2), 128–146.

Haunschild, P. R., & Miner, A. S. (1997). Modes of inter-organizational imitation: The effects of outcome salience and uncertainty. *Administrative Science Quarterly*, *42*(3), 472.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY: Guilford Press.

Hettinger, E. (1989). Justifying intellectual property. *Philosophy & Public Affairs*, *18*(1), 31–52.

Hill, J. A., Eckerd, S., Wilson, D., & Greer, B. (2009). The effect of unethical behavior on trust in a buyer–supplier relationship: The mediating role of psychological contract violation. *Journal of Operations Management*, *27*(4), 281–293.

Hoecht, A., & Trott, P. (2006). Outsourcing, information leakage and the risk of losing technology-based competencies. *European Business Review*, *18*(5), 395–412.

Hora, M., & Klassen, R. D. (2013). Learning from others' misfortune: Factors influencing knowledge acquisition to reduce operational risk. *Journal of Operations Management*, *31*(1–2), 52–61.

Hu, L.-T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55.

Huang, S., Guan, X., & Chen, Y. J. (2018). Retailer information sharing with supplier encroachment. *Production and Operations Management*, *27*(6), 1133–1147.

Husted, K., & Michailova, S. (2010). Dual allegiance and knowledge sharing in inter-firm R&D collaborations. *Organizational Dynamics*, *39*(1), 37–47.

Ireland, R. D., & Webb, J. W. (2007). A multi-theoretic perspective on trust and power in strategic supply chains. *Journal of Operations Management*, *25*(2), 482–497.

Jain, A., & Sohoni, M. (2015). Should firms conceal information when dealing with common suppliers? *Naval Research Logistics*, *62*(1), 1–15.

Johnston, D. A., McCutcheon, D. M., Stuart, F. I., & Kerwood, H. (2004). Effects of supplier trust on performance of cooperative supplier relationships. *Journal of Operations Management*, *22*(1), 23–38.

Kaufmann, L., Esslinger, J., & Carter, C. R. (2018). Toward relationship resilience: Managing buyer-induced breaches of psychological contracts during joint buyer–supplier projects. *Journal of Supply Chain Management*, *54*(4), 62–85.

Ketokivi, M., & McIntosh, C. N. (2017). Addressing the endogeneity dilemma in operations management research: Theoretical, empirical, and pragmatic considerations. *Journal of Operations Management*, *52*(1), 1–14.

Kim, J.-Y., & Miner, A. S. (2007). Vicarious learning from the failures and near-failures of others: Evidence from the U.S. commercial banking industry. *Academy of Management Journal*, *50*(3), 687–714.

Kim, P. H., Dirks, K. T., Cooper, C. D., & Ferrin, D. L. (2006). When more blame is better than less: The implications of internal vs. external attributions for the repair of trust after a competence- vs. integrity-based trust violation. *Organizational Behavior and Human Decision Processes*, *99*(1), 49–65.

Kong, G., Rajagopalan, S., & Zhang, H. (2013). Revenue sharing and information leakage in a supply chain. *Management Science*, *59*(3), 556–572.

Kong, G., Rajagopalan, S., & Zhang, H. (2017). Information leakage in supply chains. In A. Y. Ha & C. S. Tang (Eds.), *Handbook of information exchange in supply chain management* (Vol. 5, pp. 313–341). Cham: Springer Series in Supply Chain Management.

Kovach, K. A., Pruett, M., Samuels, L. B., & Duvall, C. F. (2004). Protecting trade secrets during employee migration: What you don't know can hurt you. *Labour Law Journal*, *55*(2), 69–84.

Krypotos, A.-M., Effting, M., Kindt, M., & Beckers, T. (2015). Avoidance learning: A review of theoretical models and recent developments. *Frontiers in Behavioral Neuroscience*, *9*, 1–16.

Kurtuluş, M., & Toktay, L. B. (2009). Category captainship practices in the retail industry. In N. Agrawal & S. A. Smith (Eds.), *Retail supply chain management: Quantitative models and empirical studies* (pp. 79–98). New York: Springer.

Lawson, B., Tyler, B. B., & Cousins, P. D. (2008). Antecedents and consequences of social capital on buyer performance improvement. *Journal of Operations Management*, *26*(3), 446–460.

Lee, Y. S., Seo, Y. W., & Siemsen, E. (2018). Running behavioral operations experiments using Amazon's mechanical Turk. *Production and Operations Management*, *27*(5), 973–989.

Lejeune, M. A., & Yakova, N. (2005). On characterizing the 4 C's in supply chain management. *Journal of Operations Management*, *23*(1), 81–100.

Li, L. (2002). Information sharing in a supply chain with horizontal competition. *Management Science*, *48*(9), 1196–1212.

Li, S., & Lin, B. (2006). Accessing information sharing and information quality in supply chain management. *Decision Support Systems*, *42*(3), 1641–1656.

Loch, C. H. (2017). Creativity and risk taking aren't rational: Behavioral operations in MOT. *Production and Operations Management*, *26*(4), 591–604.

Loch, C. H., & Wu, Y. (2008). Social preferences and supply chain performance: An experimental study. *Management Science*, *54*(11), 1835–1849.

Lumineau, F., Eckerd, S., & Handley, S. (2015). Inter-organizational conflicts: Research overview, challenges, and opportunities. *Journal of Strategic Contracting and Negotiation*, *1*(1), 42–64.

March, J. G. (1991). Exploration and exploitation in organizational learning. *Organization Science*, *2*(1), 71–87.

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's mechanical Turk. *Behavior Research Methods*, *44*(1), 1–23.

Massimino, B., Gray, J. V., & Lan, Y. (2018). On the inattention to digital confidentiality in operations and supply chain research. *Production and Operations Management*, *27*(8), 1492–1515.

Mayer, R. C., & Davis, J. H. (1999). The effect of the performance appraisal system on trust for management: A field quasi-experiment. *Journal of Applied Psychology*, *84*(1), 123–136.

McGrath, J. E. (1982). Dilemmatics: The study of research choices and dilemmas. In J. E. McGrath, J. Martin, & R. A. Kulka (Eds.), *Judgment calls in research* (pp. 69–102). Beverly Hills, CA: Sage Publications.

Mena, C., Humphries, A., & Choi, T. Y. (2013). Toward a theory of multi-tier supply chain management. *Journal of Supply Chain Management*, *49*(2), 58–77.

Menges, J. I., & Kilduff, M. (2015). Group emotions: Cutting the Gordian knots concerning terms, levels of analysis, and processes. *The Academy of Management Annals*, *9*(1), 845–928.

Mir, S., Aloysius, J. A., & Eckerd, S. (2016). Understanding supplier switching behavior: The role of psychological contracts in a competitive setting. *Journal of Supply Chain Management*, *53*(3), 3–18.

Mohr, J., & Spekman, R. (1994). Characteristics of partnership success: Partnership attributes, communication behavior, and conflict resolution techniques. *Strategic Management Journal*, *15*(2), 135–152.

Moorman, C., & Miner, A. S. (1997). The impact of organizational memory on new product performance and creativity. *Journal of Marketing Research*, *34*(1), 91–106.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, *58*(3), 20–38.

Narasimhan, R., Nair, A., Griffith, D. A., Arlbjørn, J. S., & Bendoly, E. (2009). Lock-in situations in supply chains: A social exchange theoretic study of sourcing arrangements in buyer–supplier relationships. *Journal of Operations Management*, *27*(5), 374–389.

Nyaga, G. N., Whipple, J. M., & Lynch, D. F. (2010). Examining supply chain relationships: Do buyer and supplier perspectives on collaborative relationships differ? *Journal of Operations Management*, *28*(2), 101–114.

Oflaç, B. S., Sullivan, U. Y., & Baltacioğlu, T. (2012). An attribution approach to consumer evaluations in logistics customer service failure situations. *Journal of Supply Chain Management*, *48*(4), 51–71.

Okleshen, M., & Hoyt, R. (1996). A cross-cultural comparison of ethical perspectives and decision approaches of business students: United States of America versus New Zealand. *Journal of Business Ethics*, *15*(5), 537–549.

Özer, Ö., Zheng, Y., & Chen, K. Y. (2011). Trust in forecast information sharing. *Management Science*, *57*(6), 1111–1137.

Pandey, V. C., Garg, S. K., & Shankar, R. (2010). Impact of information sharing on competitive strength of Indian manufacturing enterprises. *Business Process Management Journal*, *16*(2), 226–243.

Park, B. S., Park, H., & Ramanujam, R. (2018). Tua culpa: When an organization blames its partner for failure in a shared task. *Academy of Management Review*, *43*(4), 792–811.

Parkinson, M., & Byrne, R. M. J. (2018). Judgments of moral responsibility and wrongness for intentional and accidental harm and purity violations. *Quarterly Journal of Experimental Psychology*, *71*(3), 779–789.

Peer, E., Vosgerau, J., & Acquisti, A. (2014). Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior Research Methods*, *46*(4), 1023–1031.

Polyviou, M., Rungtusanatham, M. J., Reczek, R. W., & Knemeyer, A. M. (2018). Supplier non-retention post disruption: What role does anger play? *Journal of Operations Management*, *61*(1), 1–14.

Poppo, L., Zhou, K. Z., & Ryu, S. (2008). Alternative origins to interorganizational trust: An interdependence perspective on the shadow of the past and the shadow of the future. *Organization Science*, *19*(1), 39–55.

Pratt, M. G. (2008). Fitting oval pegs into round holes: Tensions in evaluating and publishing qualitative research in top-tier North American journals. *Organizational Research Methods*, *11*(3), 481–509.

Pratt, M. G. (2009). From the editors: For the lack of a boilerplate: Tips on writing up (and reviewing) qualitative research. *Academy of Management Journal*, *52*(5), 856–862.

Price, L. L., & Arnould, E. J. (1999). Commercial friendships: Service provider–client relationships in context. *Journal of Marketing*, *63*(4), 38–56.

Rand, D. G. (2012). The promise of mechanical Turk: How online labor markets can help theorists run behavioral experiments. *Journal of Theoretical Biology*, *299*, 172–179.

Razzaque, M. A., & Hwee, T. P. (2002). Ethics and purchasing dilemma: A Singaporean view. *Journal of Business Ethics*, *35*(4), 307–326.

Reeder, G. D., & Brewer, M. B. (1979). A schematic model of dispositional attribution in interpersonal perception. *Psychological Review*, *86*(1), 61–79.

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation*, *35*, 22–31.

Rizvi, S., & Bobocel, D. R. (2016). Promoting forgiveness through psychological distance. *Social Psychological and Personality Science*, *7*(8), 875–883.

Robinson, J. P., Shaver, P. R., & Wrightsman, L. S. (1991). Criteria for scale selection and evaluation. In J. P. Robinson, P. R. Shaver, & L. S. Wrightsman (Eds.), *Measures of personality and social psychological attitudes* (pp. 1–16). San Diego, CA: Academic Press.

Rogers, Z., Benjamin, V., & Gopalakrishnan, M. (2018). *Cyber security in supply chains: Understanding threats and potential security practices. Report*. Tempe, AZ: Center for Advanced Procurement Strategy.

Rungtusanatham, M., Miller, J. W., & Boyer, K. K. (2014). Theorizing, testing, and concluding for mediation in SCM research: Tutorial and procedural recommendations. *Journal of Operations Management*, *32*(3), 99–113.

Schoenherr, T., Bendoly, E., Bachrach, D. G., & Hood, A. C. (2017). Task interdependence impacts on reciprocity in IT implementation teams: Bringing out the worst in us, or driving responsibility? *Production and Operations Management*, *26*(4), 667–685.

Shah, R., & Goldstein, S. M. (2006). Use of structural equation modeling in operations management research: Looking back and forward. *Journal of Operations Management*, *24*(2), 148–169.

Shamir, N. (2017). Cartel formation through strategic information leakage in a distribution channel. *Marketing Science*, *36*(1), 70–88.

Shang, W., Ha, A. Y., & Tong, S. (2015). Information sharing in a supply chain with a common retailer. *Management Science*, *62*(1), 245–263.

Sheu, C., Yen, H. R., & Chae, B. (2006). Determinants of supplier–retailer collaboration: Evidence from an international study. *International Journal of Operations & Production Management*, *26*(1), 24–49.

Siemsen, E., Roth, A. V., Balasubramanian, S., & Anand, G. (2009). The influence of psychological safety and confidence in knowledge on employee knowledge sharing. *Manufacturing & Service Operations Management*, *11*(3), 429–447.

Simester, A. P. (2005). Responsibility for inadvertent acts. *Ohio State Journal of Criminal Law*, *2*, 601–606.

Sinkula, J. M., Baker, W. E., & Noordewier, T. (1997). A framework for market-based organizational learning: Linking values, knowledge, and behavior. *Journal of the Academy of Marketing Science*, *25*(4), 305–318.

Smith, E. R., Seger, C. R., & Mackie, D. M. (2007). Can emotions be truly group level? Evidence regarding four conceptual criteria. *Journal of Personality and Social Psychology*, *93*(3), 431–446.

Speier, C., Whipple, J. M., Closs, D. J., & Voss, M. D. (2011). Global supply chain design considerations: Mitigating product safety and security risks. *Journal of Operations Management*, *29*(7–8), 721–736.

Spiliotopoulou, E., Donohue, K., & Gürbüz, M. Ç. (2016). Information reliability in supply chains: The case of multiple retailers. *Production and Operations Management*, *25*(3), 548–567.

Swan, J. E., Goodwin, C., Mayo, M. A., & Richardson, L. D. (2001). Customer identities: Customers as commercial friends, customer coworkers or business acquaintances. *Journal of Personal Selling & Sales Management*, *21*(1), 29–37.

Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and knowledge leakage in supply chain. *Information Systems Frontiers*, *18*(3), 621–638.

Taylor, A. B., MacKinnon, D. P., & Tein, J.-Y. (2008). Tests of the three-path mediated effect. *Organizational Research Methods*, *11*(2), 241–269.

Thornton, R. A., & Thompson, P. (2001). Learning from experience and learning from others: An exploration of learning and spillovers in wartime shipbuilding. *American Economic Review*, *91*(5), 1350–1368.

Urda, J., & Loch, C. H. (2013). Social preferences and emotions as regulators of behavior in processes. *Journal of Operations Management*, *31*(1–2), 6–23.

Villena, V. H., Revilla, E., & Choi, T. Y. (2011). The dark side of buyer–supplier relationships: A social capital perspective. *Journal of Operations Management*, *29*(6), 561–576.

Wason, K. D., Polonsky, M. J., & Hyman, M. R. (2002). Designing vignette studies in marketing. *Australasian Marketing Journal*, *10*(3), 41–58.

Weick, K. E., & Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly*, *38*(3), 357–381.

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological Review*, *92*(4), 548–573.

Weiner, B. (1986). An attributional theory of achievement motivation and emotion. In *An attributional theory of motivation and emotion, SSSP springer series in social psychology*. New York, NY: Springer.

Weiner, B. (1995). *Judgments of responsibility: A foundation for a theory of social conduct*. New York, NY: Guilford Press.

Wentzel, D. (2009). The effect of employee behavior on brand personality impressions and brand attitudes. *Journal of the Academy of Marketing Science*, *37*(3), 359–374.

Williamson, O. E. (1985). *The economic institutions of capitalism: Firms, markets, relational contracting*. New York, NY: The Free Press.

Zhang, D. Y., Cao, X., Wang, L., & Zeng, Y. (2012). Mitigating the risk of information leakage in a two-level supply chain through optimal supplier selection. *Journal of Intelligent Manufacturing*, *23*(4), 1351–1364.

Zilberman, P., Katz, G., Shabtai, A., & Elovici, Y. (2013). Analyzing group E-mail exchange to detect data leakage. *Journal of the American Society for Information Science and Technology*, *64*(9), 1780–1790.

SUPPORTING INFORMATION

Additional supporting information may be found online in the Supporting Information section at the end of this article.

How to cite this article: Ried L, Eckerd S, Kaufmann L, Carter C. Spillover effects of information leakages in buyer–supplier–supplier triads. *J Oper Manag*. 2020;1–27. https://doi.org/10.1002/joom.1116

APPENDIX A: Vignettes

Introductory text (identical across all treatments)

The following short scenario describes your role as the *representative of a supplier*. Please carefully read the scenario, and try to imagine how you would *feel* and what *actions* you would take based on the presented situation. Assume that all the given information is true.

You are **the representative of SPLR**, a large-sized **battery supplier** for smartphones. In your role, you are responsible for the sales of the batteries, as well as the corresponding relationship management with your buying firms. SPLR supplies its batteries to a wide span of business customers, ranging from small- to large-sized companies that integrate SPLR's batteries in various different phones. Your company is well-known and has been an established and successful player in the industry for over a decade. For a few years now, your firm has been supplying batteries to a number of smartphone

manufacturers, including the **electronics company BYR**. BYR offers a wide range of electronic products, including smartphones and drones, among others. Similar to your firm (SPLR), BYR is a well-known and successful large-sized company with over a decade of experience in the industry. BYR's products are known to be long-lasting and of high technological quality. Your firm (SPLR) and BYR value the rather **cooperative nature of your relationship** and you have reasonably strong relational ties which are built on mutual trust. You would consider your business relationship to be mutually beneficial and solid. **However, both firms are not overly dependent on each other,** which is why SPLR and BYR have established approximately equal bargaining power in negotiations during the last few years. Terminating the relationship with BYR would take you some effort, but would not necessarily hurt your company's operations in the long-term.

BYR has never failed to follow through on any of its written or verbal commitments with SPLR and there is **no reason to believe that BYR ever acted opportunistically or deceitfully** towards your firm or any other firm in the industry. Your firm and other companies in the market would describe BYR as generally being just and understanding towards other firms. BYR is also known for its sustainability agenda, which includes a substantial reduction of plastic usage in BYR's products, as well as an increase of ethical standards regarding labor laws in emerging countries in the upcoming years. Due to technical adjustments that BYR had to make in order to ensure the compatibility of one of its phones with SPLR's battery, as well as environmental regulations that BYR had to fulfill regarding the use of certain materials in its smartphone components, your firm (SPLR) has been **sharing data about its battery and production processes** with BYR. Sharing such information is essential for many similar business collaborations in order to ensure the successful alignment between the buyer- and the supplier-side, without which no sales would be possible. As is common practice in the industry, **SPLR and BYR signed a non-disclosure agreement at the beginning** of the relationship to prevent the distribution of sensitive data with other firms.

Treatment scenario—Opportunistic [Inadvertent] and Similarity {Dissimilarity}

Last week, you learned and were able to verify from a highly reliable source that your buyer BYR **deliberately [accidentally]** emailed sensitive information to a prospective industry customer of BYR about OTS, which is one of BYR's other suppliers. **Like {Unlike}** your firm (SPLR), OTS is **also a supplier of batteries {a supplier of cameras}**. For several years now, OTS has been supplying **batteries {cameras}** as a component of one of BYR's other products, a drone. Your firm (SPLR) and OTS know each other, but there is no existing relationship between your two firms (i.e., neither cooperative nor adversarial), **although you supply similar {as you supply dissimilar}** product components. Importantly, SPLR and OTS are not competitors, since SPLR and OTS supply components for different end products (smartphone and drone, respectively) and do not intend to enter each other's businesses in the future. Buyer BYR and supplier OTS signed a non-disclosure agreement in the beginning of their relationship to prevent the sharing of sensitive information with other firms. You learned and can assume it is true that BYR's e-mail containing the sensitive information about OTS was **intentionally [unintentionally]** sent to BYR's prospective industry customer, due to **high financial gains offered from the prospective industry customer to BYR for sharing OTS's sensitive information**. **The purpose of BYR's e-mail was to show this prospective industry customer the technical details of OTS's drone battery as well as its production processes. [a mix-up of recipients in the address field by BYR. The actual purpose of BYR's e-mail was for the internal usage within BYR, which would have been in accordance with the signed non-disclosure agreement with OTS.]** This event hurts OTS in several different ways, including a substantial loss of its competitive advantage and as a result, a significant loss of its market share to other drone battery suppliers (although SPLR does not benefit, because you are not competitors). The retributions stated in the non-disclosure agreement regarding the unauthorized sharing of sensitive information offset only a minor part of OTS's damage.

APPENDIX B: Instruction and manipulation checks

Instruction Check 1
You are the representative of SPLR, a ...

a. battery supplier.
b. drone supplier.
c. smartphone manufacturer.
d. drone manufacturer.

Instruction Check 2
SPLR has been sharing information with BYR about SPLR's ...

a. employees and turnover rates.
b. product and production processes.
c. sales figures and cost structures.
d. digitalization strategy.

Manipulation Check 1
BYR's act of sharing sensitive information about OTS was intentional.
(1 = strongly disagree, 7 = strongly agree)
Manipulation Check 2
Your firm (SPLR) and OTS both supply batteries to BYR.
(1 = strongly disagree, 7 = strongly agree)

APPENDIX C: Items with standard errors and standardized loadings

Items	SE	Std. load.
Integrity-based trust		
I1: BYR [=name of buying firm] has a strong sense of justice.	0.059	0.914
I2: My firm never has to wonder whether BYR will stick to its word.	0.164	0.705
I3: BYR tries to be fair in dealings with other firms.	0.044	0.947
I4: BYR's actions and behaviors are not very consistent. *(reverse-coded)*	0.146	0.785
I5: My firm likes BYR's values.	0.033	0.961
I6: Sound principles seem to guide BYR's behavior.	0.034	0.973
Ability-based trust		
I1: BYR is very capable of performing its job.	0.102	0.773
I2: BYR is known to be successful at the things it tries to do.	0.062	0.803
I3: BYR has much knowledge about the work that needs done.	0.064	0.774
I4: My firm feels very confident about BYR's skills.	0.092	0.833
I5: BYR has specialized capabilities that can increase my firm's performance.	0.106	0.667
I6: BYR is well-qualified.	0.073	0.823
Information sharing willingness		
I1: My firm SPLR is willing to share sensitive information about SPLR's products with BYR in the future.	0.025	0.978
I2: My firm SPLR is willing to share sensitive information about SPLR's production processes with BYR in the future.	0.025	0.984
I3: My firm SPLR is willing to provide BYR with information in the future that might help them.	0.056	0.907

(Continues)

APPENDIX D: Interview questions

1. Have you ever experienced a situation where one of your customers/buying firms leaked sensitive information about your firm to an unauthorized party? Could you please describe this situation?
2. Have you experienced, heard of or read about a situation where your buying firm leaked confidential information about another supplier to an unauthorized party? What was the situation about?
3. What do you think was the intentionality behind that information leakage?
4. How long have your own firm and the buying firm been in a business relationship before this information leakage happened and how would you describe the trust level between your two firms prior to the event? How did that trust level change after your buying firm leaked information about this victim supplier?
5. When considering two dimensions of trust, "integrity-trust" and "ability-trust", how did their levels change towards the buying firm in your last information leakage example?
6. Regarding information leakages, what are your expectations about the buying firm's future behavior?
7. How did your willingness to share information with that buyer change from before to after the event? How would this depend on the type of information being shared?
8. To what extent would things surrounding the incident change for you, had your firm and the victim supplier been more (less) similar to each other?

APPENDIX E: Interviewee demographics

Reference	Sales position	Gender	Work experience	Industry	Country
Supplier 1	Vice President	Male	16 years	Construction & Mining	Germany
Supplier 2	Head of Sales	Male	17 years	Construction & Mining	Italy
Supplier 3	Senior Key Account Manager	Male	30 years	Chemical	United Kingdom
Supplier 4	General Manager	Female	12 years	Medical technology	India
Supplier 5	Senior Director	Male	18 years	Consumer goods	United States
Supplier 6	Country Manager	Male	36 years	Chemical	UK
Supplier 7	Key Account Manager	Male	25 years	Chemical	Italy
Supplier 8	Business Manager	Male	19 years	Chemical	Germany

APPENDIX F: Proof quotes

Examples of inadvertent information leakages	*Reference*
"I've got a couple of examples where I'd be passed orders which was for a competitive product and should have gone to a competitor, to their ordering system. But our customer sent it to [interviewee company] by mistake, by like email or whatever. ...It would have the product codes on, and the pricing and delivery times, payment types and all things like this."	Supplier 3
"...there are several different points where leakage can happen.... It could be a third party who is managing display execution in a store who actually has ownership over five different retail chains in the marketplace. So they hear information from one, it could easily be leaked to the other four, because they are in those same stores and they might be talking to different people and giving them notice about what they are hearing is going to be happening in the market place. So, we hear a lot about that."	Supplier 5
Examples of opportunistic information leakages	*Reference*
"The company where I was working before had very close contact with the customer and there was one guy that was almost living at the customer plant. And okay, sometimes this guy was able to get some information about what the competitors were doing. This was the practice of the company and it was not so uncommon. I know it's not allowed, but it was happening."	Supplier 2
"...We have a large customer and they want us to improve our product and they received a product from a competitor which, to them, is behaving very good and how they would want our product to be working. Now, because we have a good relationship with our customer, the production manager would tell me the price of this product and he would also offer a data sheet and he would also offer even a sample for us to test."	Supplier 3
"...In the medical device space, a lot of the selling does not go directly to the hospital; we have to supply through the distributor. So I would have probably been an observer to a situation where a distributor is sharing confidential information which again would be along the lines of product information or pricing information from another supplier to a third party. ...sometimes there is obviously a financial motive behind some of this."	Supplier 4
Inadvertent information leakage—Reduced ability-based trust	*Reference*
"It's a little bit incompetent to send such sensitive information to the wrong company. And therefore I would... question that person's ability to make sure everything is done [correctly]."	Supplier 3
Inadvertent information leakage—Reduced integrity-based trust	*Reference*
"I think both of these dimensions would be impacted negatively. Principally because we would see that the customer did not have appropriate systems in place to prevent that accidental release and therefore, they do not have systems so they are not really thinking about that integrity part."	Supplier 6
Opportunistic information leakage—Reduced ability-based trust	*Reference*

"...it undermines what I think of his knowledge and technical skills."	Supplier 3
"...they need to use that leakage of information to reach their objective and do not have the capability to reach those objectives without giving that information away."	Supplier 6
Opportunistic information leakage—Reduced integrity-based trust	*Reference*
"...this would put in question the loyalty or the integrity."	Supplier 1
"On the integrity side I question if he would pass on so easily my information to somebody else. And therefore I would be... a bit more guarded to share too much information in the future."	Supplier 3
"You´re always concerned that the same thing could happen to you. ...there is fear. ...from my personal experience integrity trust is what I would be looking for."	Supplier 4
"It really is about integrity and if you can trust that people will treat your information as their own and not leverage it in the market place or not put it in people´s hands that increase the risks."	Supplier 5
"You know, he would use the information we gave him and give that to the competitor, so I would say the integrity trust at some point would be lost."	Supplier 6