

# Guarding knowledge: Karachi Green Line Metrobus perspectives on leakage and protection

Rehab Iftikhar

*Department of Industrial and Information Management, Tampere University,  
Tampere, Finland*

Received 15 March 2025  
Revised 9 August 2025  
28 October 2025  
21 December 2025  
27 February 2026  
Accepted 22 March 2026

## Abstract

**Purpose** – This paper aims to consider how knowledge leakage occurs, as well as how that knowledge can be protected, particularly when it pertains to interorganizational projects. This is a case study on the Green Line Metrobus in Karachi, Pakistan.

**Design/methodology/approach** – This paper uses a single case study approach. Data was collected through semistructured interviews and archival documents. Data analysis was conducted using thematic analysis.

**Findings** – The findings present the determinants of knowledge leakage, employee mobility, information disorder, misuse of knowledge-sharing tools and diverse stakeholders' involvement. For knowledge protection, the findings provide evidence of nondisclosure agreements, standard operating procedures, education and training and sharing relevant knowledge.

**Originality/value** – By examining knowledge leakage and protection in interorganizational projects, this study contributes to the literature on protection motivation theory. Furthermore, it offers practical insights for practitioners to better understand and mitigate knowledge leakage through effective knowledge protection mechanisms.

**Keywords** Knowledge leakage, Knowledge protection, Interorganizational projects

**Paper type** Research paper

## Introduction

Knowledge resides not just within organizational boundaries but also outside of them (Silva, Howell, & Meyer, 2018), specifically in internal networks and external networks (Iftikhar & Ahola, 2022). Organizations use outside sources to get meaningful knowledge; in particular, they require complementary external skills to assist them in solving novel issues. External knowledge can be integrated with internal knowledge to generate new ideas and capabilities that can boost an organization's competitive advantage (Argote, McEvily, & Reagans, 2003). In interorganizational projects, numerous organizations aim to assimilate useful knowledge and gain competence from one another (Hamel, 1991), as well as to acquire valuable external knowledge across fields (Love, Roper, & Vahter, 2014; Magni, Chierici, Fait, & Lefebvre, 2022). An organization faces an inherent risk if it shares too much project-specific knowledge with other organizations. When valuable organizational knowledge leaks, it can erode competitive advantages (Spender, 1996; Ritala, Olander, Michailova, & Husted, 2015).



In an interorganizational project, organizations collaborate to produce a desired product or service that cannot be achieved by individual organizations (Iftikhar & Ahola, 2022), which facilitates knowledge sharing (Estrada, Faems, & de Faria, 2016) but can also lead to knowledge leakages (Ritala, Kenneth, Heidi, & Snejina, 2018). Knowledge leakage occurs when an organization loses vital knowledge to others, resulting in lower organizational performance (Easterby-Smith, Lyles, & Tsang, 2008). Some organizations use knowledge protection measures, particularly in the context of coopetition (Balle, Steffen, Curado, & Oliveira, 2019; Estrada et al., 2016), such as interorganizational initiatives. An organization's ability to protect its knowledge enhances its competitive advantage through both formal and informal protection mechanisms (Balle et al., 2019). The coopetition perspective posits that cooperation and competition function simultaneously in interorganizational projects (Lado, Boyd, & Hanlon, 1997; Li, Liu, & Liu, 2011), which gives access to resources and knowledge (Enberg, 2012; Gast, Gundolf, Harms, & Collado, 2019). Organizations collaborating with different heterogeneous partners may also face the risk of losing their innovative knowledge during collaboration (Chen, Yao, Zan, & Carayannis, 2021; Wang, Chin, Chiew, & Capalbo, 2024). Consequently, organizations may be prone to knowledge leakage if their partners have incentives to appropriate their proprietary knowledge (Heiman & Nickerson, 2004; Jiang, Li, Gao, Bao, & Jiang, 2013). Knowledge protection, however, presents a paradox: organizations may be underprotected by sharing too much knowledge, thereby losing their competitive advantage, or they may be overprotected by sharing too little knowledge, weakening the positive effects of knowledge sharing (Frishammar, Ericsson, & Patel, 2015).

Moreover, knowledge is classified into explicit and tacit knowledge (Shujahat et al., 2017). Explicit knowledge may easily be formalized, reproduced and replicated across an organization. Tacit knowledge is embedded in an organization's culture, making it difficult to codify (i.e. to duplicate, replicate or transfer from one organization to another). It is outside the scope of this study to engage with knowledge categories; however, current research suggests that tacit knowledge is less susceptible to leakages than explicit knowledge (Nonaka & Von Krogh, 2009; Wu & Lin, 2013). While both explicit and tacit knowledge are valuable to organizations involved in interorganizational projects, explicit knowledge is a critical source of competitive advantage since it can be sold to other organizations and easily transferred from one to another. Therefore, sharing tacit knowledge assets is very helpful, and partnering organizations must have access to tacit knowledge to add value to their collaboration. However, providing such access raises the possibility of opportunism (Ritala et al., 2015; Solli-Sæther, Karlsen, & van Oorschot, 2015). To avoid confusion, we will use the general term knowledge throughout the study.

Knowledge leakage can be positive or negative, depending on whether it benefits or harms the organization (Grillitsch & Nilsson, 2017; Jiang, Bao, Xie, & Gao, 2016). Prior research has predominantly emphasized its negative consequences, including damage to innovation, performance, reputation and financial outcomes (Frishammar et al., 2015; Flammer & Kacperczyk, 2019; Ritala et al., 2015, 2018). Existing studies identify sources such as social media and mobile technologies (Durst, Aggestam, & Ferenhof, 2015; Yahav, Schwartz, & Silverman, 2014), as well as organizational change, retirement and turnover (Carmel, Pak, & Patel, 2013; Chalkiti & Sigala, 2010; Treleven & Sykes, 2005). Knowledge protection is critical to preserving the interests, creativity, legal rights and patents of knowledge owners (Balle et al., 2019). Knowledge protection mechanisms – such as contracts, social governance and trust – are therefore essential, particularly in interorganizational contexts where employees play a central role in preventing knowledge leakage (Ritala et al., 2015; Charterina, Basterretxea, & Landeta, 2017). Knowledge leakage

and protection have been studied in the context of multinational companies (de Faria & Sofka, 2010), high technical organizations (Solli-Sæther et al., 2015), the construction industry and defense organizations (Hernandez, Sanders, & Tuschke, 2015; Sharif, Naiding, Xu, & Rehman, 2020).

The study of knowledge leakage and protection in interorganizational projects appears to be underdeveloped, as stated earlier. In particular, for infrastructural projects, design information, technical and financial ideas have been found to be the most prone to leakage. As a result, organizations must protect their collaborative projects from the danger of knowledge leaking (Sharif et al., 2020). However, contemporary research has not explained how concrete leakage mechanisms and protection practices interact in interorganizational infrastructure projects; this study addresses this gap by empirically linking leakage sources and protection mechanisms to threat and coping responses through the lens of protection motivation theory (PMT). Hence, this research unpacks knowledge leakage and protection in an interorganizational project by answering the following research questions:

RQ1. How does knowledge leakage occur in an interorganizational project?

RQ2. How do organizations protect knowledge in an interorganizational project?

From a learning-organization perspective, interorganizational projects function as distributed learning systems where multiple organizations jointly create and apply knowledge. Consequently, examining knowledge leakage and protection is essential for understanding how learning organizations (interorganizational projects) balance openness for learning with the need to retain and institutionalize critical knowledge. An interorganizational project is analyzed as a unit of analysis because it allows multiple organizations to work together toward the same objective. The Green Line (GL) Metrobus in Pakistan, which is an interorganizational project, was examined. This study makes two contributions. The first contribution is to provide insights into knowledge leakage in an interorganizational project. The second contribution is to provide knowledge protection strategies.

## Literature review

### *Knowledge leakage*

Knowledge leakage is defined as “the extent to which the focal organization’s private knowledge is intentionally appropriated by or unintentionally transferred to partners beyond the scope of the alliance agreement” (Jiang et al., 2013: p. 984). It refers to the flow of knowledge beyond organizational boundaries, resulting in the deterioration of competitiveness and of the organization’s industrial position (Frishammar et al., 2015; Flammer & Kacperczyk, 2019; Ritala et al., 2018). To understand knowledge leakage, it is essential to distinguish between public and private knowledge. Public knowledge exists in the public domain and is accessible to multiple organizations, whereas private knowledge is organization-specific and intended to remain within organizational boundaries (Matusik & Hill, 1998; Frishammar et al., 2015). In the interorganizational setting, public knowledge is not exclusive; organizations can access and apply it. In contrast, the focal organization only holds private knowledge, which provides the possessor with a competitive advantage (Tiwana, 2008), but it also presents a high risk of knowledge leakage.

Intentional knowledge leakage involves deliberate actions by individuals or organizations that expose proprietary knowledge to external parties (Ritala et al., 2015), often driven by opportunistic behavior such as unauthorized imitation or private learning. In such cases, partners may seek appropriate valuable knowledge to outperform collaborators or pursue hidden agendas (Das & Teng, 2001; Jiang et al., 2013). Unintentional knowledge leakage, by

contrast, occurs when organizations unknowingly transfer knowledge beyond agreed boundaries, typically through frequent interactions and communication across project networks (Kale, Singh, & Perlmutter, 2000; Mohr & Sengupta, 2002). This form of leakage often arises when employees are unclear about what information can be shared, leading to accidental disclosures, particularly through informal contacts and communication channels (Arias-Pérez, Lozada, & Henao-García, 2020; Jiang et al., 2013).

Interorganizational projects provide a fertile context for knowledge leakage. These projects are complex and time-bound collaborations in which organizations pool specialized skills, technologies and knowledge to achieve shared goals that cannot be accomplished independently (Jiang et al., 2016). While such collaboration facilitates learning and knowledge exchange, it also creates opportunities for opportunistic behavior (Walter, Walter, & Müller, 2015). Knowledge leakage occurs when partners gain access to economically valuable knowledge beyond contractual agreements, thereby threatening project autonomy and organizational advantage (Jiang et al., 2013; Chen et al., 2021; Shi, Zhang, & Zheng, 2019). The disclosure of such commercial secrets jeopardizes a project's autonomy (Shi et al., 2019). Because certain capabilities retain their value only when they remain exclusive (Ahlfänger, Gemünden, & Leker, 2022; Frishammar et al., 2015), organizations seek to control external disclosure of critical knowledge resources. Organizations are particularly cautious about sharing knowledge that underpins competitive advantage or could be leveraged by competitors (Bloodgood & Chen, 2022). Consequently, knowledge protection plays a vital role in preventing imitation and sustaining long-term competitive advantage (Frishammar et al., 2015).

### *Knowledge protection*

Knowledge protection refers to the strategies and actions organizations use to safeguard valuable knowledge assets and to prevent knowledge leakage to unauthorized individuals or entities (Manhart & Thalmann, 2015). Organizations are especially sensitive to knowledge leakage in contexts involving intensive knowledge exchange, such as interorganizational projects (Ahlfänger et al., 2022; Ritala & Hurmelinna-Laukkanen, 2013). In such settings, organizations may gain privileged access to shared knowledge bases and acquire new knowledge from partners without their consent or adequate compensation (Jaffe, Trajtenberg, & Henderson, 1993). To benefit from interorganizational relationships, organizations must therefore carefully decide what knowledge to share, with whom and how to protect knowledge they wish to retain (Gast et al., 2019). In interorganizational projects, organizations often safeguard their resources (Andersén, 2012; Hamel, Doz, & Prahalad, 1989) and “protect information from bleeding through to a partner” (Hamel, 1991: 96) to prevent the leakage of knowledge. Knowledge protection generally focuses on two objectives: preventing unauthorized access to knowledge (Manhart & Thalmann, 2015); and reducing knowledge visibility, that is, the extent to which external parties can observe and appropriate knowledge (Lee, Chang, Liu, & Yang, 2007). However, knowledge protection is challenging for two main reasons. First, protecting explicit knowledge through property rights is costly and difficult to enforce (Chan & Lee, 2011). Second, tacit knowledge is complex, context-specific and embedded in individuals, making it difficult to codify or legally protect (DeSouza, 2006; Nelson & Winter, 1982). As a result, organizations rely on a combination of formal and informal mechanisms to retain proprietary knowledge within organizational boundaries (Ritala, Kianto, Vanhala, & Hussinki, 2023; Thomä & Bizer, 2013), particularly in interorganizational settings (Estrada et al., 2016; Fernandez & Chiambaretto, 2016).

Formal knowledge protection mechanisms include intellectual property rights and contracts, such as patents, trademarks, copyrights, trade secrets and confidentiality agreements (Olander, Vanhala, & Hurmelinna-Laukkanen, 2014). These mechanisms allow organizations to protect innovations and delay imitation, but have notable limitations. Acquiring formal protection is often resource-intensive, time-consuming and costly, frequently requiring legal expertise (de Faria & Sofka, 2010; Leiponen & Byma, 2009). Moreover, formal protection may require disclosure of information, for example, patent filings make knowledge publicly accessible, enabling competitors to imitate or build upon it (Somaya, 2003; Olander et al., 2014). Excessive reliance on contracts may also signal distrust and negatively affect interorganizational relationships (Malhotra & Murnighan, 2002). Despite these drawbacks, formal mechanisms are particularly effective for protecting codified knowledge embedded in products or services (Estrada et al., 2016; James, Leiblein, & Lu, 2013).

Since formal protection measures cannot entirely protect knowledge, as knowledge leakage beyond formal bounds may continue, informal protection supplements formal protection (Gast et al., 2019). Informal mechanisms emphasize relational governance, including trust, shared norms, reputation and human resource management practices (Fernandez & Chiambaretto, 2016; Jiang et al., 2013). Personal ties and relational standards can discourage opportunistic behavior and reduce the likelihood of imitation (Solli-Sæther et al., 2015). Although tacit knowledge is difficult to legally protect, its inherent complexity and limited transferability provide a natural form of protection (Olander et al., 2014). Together, formal and informal mechanisms enable organizations to balance knowledge sharing and protection in interorganizational projects.

#### *Interorganizational projects*

Interorganizational projects involve numerous organizations working together on common tasks over a certain time to coordinate the provision of complex products, subsystems and services (Roehrich, Kalra, Squire, & Davies, 2023). They have a distinct organizational structure with strong temporal bounds, involving collaborations among multiple organizations for a highly tailored goal that may benefit society as a whole (Fernandes, Wegner, & Möllering, 2023; Manning, 2017). An interorganizational network achieves outcomes that would not have been possible if each organization operated independently. A project requires the collaboration and pooling of resources and the expertise of various organizations (Oliveira & Lumineau, 2017). In an integrated effort to produce a product or service, each organization focuses on its own distinctive competencies, while the others focus on complementary activities (Barringer & Harrison, 2000). By virtue of its complementarities, an interorganizational project thus entails an interaction between organizations (Braun & Sydow, 2019). Interorganizational projects involve the collaboration of several legally independent but functionally interdependent organizations to accomplish a complex product or service (Lumineau & Oliveira, 2018).

#### *Protection motivation theory*

PMT assists individuals and organizations in responding, when faced with a threat, to protect themselves (Anderson & Agarwal, 2010). According to PMT, individuals and organizations protect themselves by assessing the threat and their coping capacities. The threat appraisal evaluates the severity of the situation and determines how serious it is. A threat appraisal is based on the perceived severity of a threatening event and its probability of occurrence. The coping appraisal examines how the individual and the organization respond to the situation. It produces the expectation that a recommended action will remove or reduce a threat, based

on the perception of reaction efficacy (Rogers, 1975). Threat appraisals motivate individuals and organizations to respond to situations to minimize the threat (Rippetoe & Rogers, 1987). The lens of PMT is used (Anderson & Agarwal, 2010; Rogers, 1975) to rethink knowledge leakage as a threat and knowledge protection as a coping behavior.

## Methodology

### Research design

This study adopts a single case study approach to develop an in-depth understanding of knowledge leakage and protection in an interorganizational project. The case study method is well suited to addressing research questions that require rich, contextual insight (Hartley, 2004). The GL Metrobus project in Karachi involves multiple organizations and intensive cross-boundary knowledge exchange, making it a suitable case for examining how knowledge leakage occurs and how it is addressed through protection mechanisms. The research questions are addressed through an inductive approach.

### Case context

*Karachi: green line metrobus.* The GL commences in Karachi. GL is about 23.2 km long and includes 10.5 km of elevated track and 9.3 km at grade, with a total of 25 stations. GL is designed to carry up to 30,000 passengers per hour in each direction. Each day, approximately 300,000 passengers are supposed to travel on GL. The project cost Rs. 35bn (US\$250m). The project's execution commenced in February 2016. Approximately half of Karachi's population relies excessively on private transportation, leading to traffic jams and severe environmental pollution. Traffic congestion is primarily caused by inadequate transportation infrastructure. Consequently, accessibility, health, well-being and financial services are adversely affected. However, GL has improved the quality of travel by providing a decent, comfortable, environmentally friendly and affordable bus service.

The project is comprised of different organizations consisting of a client, a design consultant, an engineering consultant, an operating consultant, a sponsoring agency (a foreign-based organization), an executing agency, contractors and a digital marketing agency. GL was initially divided into 20 packages (subprojects); however, 2 packages were cancelled. The civil work is divided into nine packages (subprojects), the electronic and mechanical works into six packages (subprojects) and the road works into three packages (subprojects), all assigned to different contractors. The project became operational in December 2021 (archival data).

### Data collection

This study used two methods of data collection. First, semistructured interviews provided the primary method of data collection, as they were able to gather rich information on relatively unexplored topics. Second, archival data was used to construct the background for the case (Yin, 2018).

Semistructured interviews are considered (see Appendix for the interview guide). Eleven interviews with 11 participants were conducted through MS Teams, ranging from 45 min to 107 min in length (details are provided in Table 1). The interviewees included project managers, the senior manager, the communication manager, the technical director and other team members (planning engineer, assistant planning engineer, digital marketing manager and transport manager). They included members of the client team, the design consultant, the operating consultant, contractors and the digital marketing agency. The interviewees were asked a series of structured and open-ended questions. Throughout the interview, interviewees were encouraged to use their own terminology and to steer the conversation

**Table 1.** Methods for data collection

Role of organization	Designations	Education	Experience (years)	Interview duration (minutes)
<i>Interviews</i>				
Client	Communication manager	MBA	11	62
	Senior manager	Masters	12	60
	Transport manager	MSc	10	107
Design consultant	Senior project manager	Masters	35	45
Operating consultant	Technical director	MSc	14	104
Contractor 1	Project manager	Masters	9	85
	Assistant planning engineer	Masters	5	68
Contractor 2	Project manager	Bachelor	8	72
	Planning engineer	BE	10	66
Contractor 3	Project manager	Masters	13	89
Digital marketing agency	Digital marketing manager	MBA	18	75
<i>Archival data</i>				
Type of archival data				Quantity
Bid evaluation reports				20
Environmental impact report and funding reports				3
Feasibility report				4
PC-1				15
Master plan				10
Topography study report				141
Traffic count				24
<i>Visual data</i>				
Videos				1
<b>Source(s):</b> Author's own work				

toward topics and concepts they felt best reflected their own experiences. The snowball sampling technique was used, in which each interviewee was asked to nominate other potential informants, those who they believed would be able to assist in understanding knowledge leakage and protection. We recorded the interviews and transcribed them.

The study also relied on archival sources of data that were provided by interviewees. A total of 218 internal and publicly accessible data are included in the archive, consisting of bid evaluation reports, environmental impact assessments, feasibility reports, topography study reports, design details (layouts and drawings) and planning commission documents. Documents were requested from the client, the contractors and the consultants. As a result of the analysis of archival data, a more detailed understanding of the case context was developed.

#### *Data analysis*

Thematic analysis was used for the analysis of the data. In thematic analysis, patterns (themes) are systematically identified and organized, and insights are provided (Braun & Clarke, 2012). In this study, the thematic analysis was highly inductive (Howitt & Cramer, 2007), and the themes identified were derived from the data itself (Braun & Clarke, 2012). In

this study, [Braun & Clarke \(2012\)](#) practical guide for applying thematic analysis was adopted. The transcriptions were first read and explored inductively to identify different methods of knowledge leakage and protection. Second, subthemes were developed, including employee mobility, information disorder, misuse of knowledge-sharing tools, diverse stakeholders' involvement, nondisclosure agreements, standard operating procedures (SOPs), education and training and sharing relevant knowledge. In the third step, the main themes were determined by reviewing the subthemes. [Table 2](#) below illustrates the analysis process of deriving the subthemes from interview transcriptions and then leading to themes.

[Figure 1](#) below will provide a step-wise analysis approach adopted for the analysis.

## Findings

The findings provide evidence of knowledge leakage and protection practices from an interorganizational project. For knowledge leakage, the subthemes of employee mobility, information disorder, misuse of knowledge-sharing tools and diverse stakeholders' involvement were found. For knowledge protection, the subthemes of nondisclosure agreements, SOPs, education and training and sharing relevant knowledge.

### *Knowledge leakage*

*Employee mobility.* Knowledge leakage occurs when an employee leaves an organization and joins another organization. Sometimes competitors try to hire employees from other organizations with the intention to benefit from knowledge leakage. As illustrated below:

During the bidding the quantity surveyor (QS) was involved, suddenly, he moved to the other organization, we didn't stop him. The other organization was also in the bidding process for the same project, as soon as he was shifted, the organization won the bid, and they were awarded with the project. Our prices were very economical [...] Upon investigation, we came to know that the bid price we had quoted was told to the other organization by our own ex-QS. (Project Manager, Contractor 3)

Moreover, there is no practice of handing over documents. If an employee is leaving, they can take documents with them and later use those documents for their own benefit. As stated below:

I left the organization, and nobody even asked me if the documents you have, do you return them to the company? Is there something in your laptop that is related to our organization, then you should delete it, or have you emailed some information to yourself, and if I'm exchanging information on my private platforms, that is very important. (Communication Manager, Client)

*Information disorder.* The media, including print, electronic and social media, is a big source of information disorder. People working on projects sometimes leak information. These may later be presented by the media in such a way as to have a negative impact on the project. General public perception can also be distorted by such actions. As illustrated below:

As I mentioned, impediments were not considered in the design phase. Now obviously, the construction team, client, consultant and contractor should have kept it between them only, but these things got leaked in media and they made NEWS that design for this project has neglected the presence of gas lines and sewerage lines. The public starts observing the project negatively, that the project is not good. (Project Manager, Contractor 3)

The media provides information without credibility. Most of the news provided is wrong, but it could cause damage to the project:

**Table 2.** Representative quotes

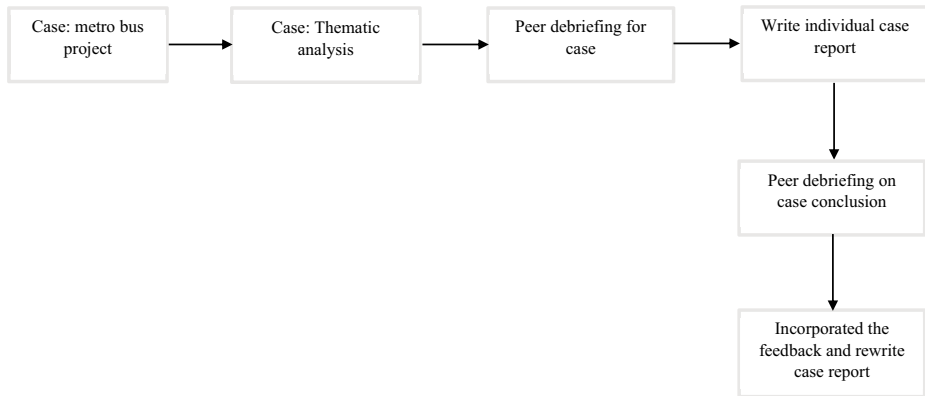
Themes	Subthemes	Initial coding	Illustrative quotes
Knowledge leakage	Employee mobility	Departing employees leave with knowledge which can be leaked	If employer leave the company, so when they are departing from one company to the other, the risk of knowledge also departs, from one company to the other. They might leak knowledge. (Project Manager, Contractor 3)
	Information disorder	Misquoting things Unreliable sources for information	Knowledge leakage occurs as the media did from visiting the site, looking at things they got to know about things, and were misquoting them. They talked to whoever would be standing over there. The media came and saw these things and highlighted them. They created a negative image. (Project Manager, Contractor 1)
	Misuse of knowledge-sharing tools	Sharing something on WhatsApp cause of leakage	There are like 10 people in WhatsApp group, and if you share something there and then that gets spread everywhere. Things get leaked. (Transport Manager, Client)
	Diverse stakeholders' involvement	Different sources of knowledge leakage Some team members act irresponsibly and spread misinformation	Some days back [project name] bus hit a column, the driver was less trained and the wind screen was damaged, it happens, it's not a big deal, all our things are insured next day, the wind screen was fixed at zero cost. I'm trying to tell you that my team started getting calls, what happened? How did it happen? So many people report it with responsibility, but one or two said that look these are so low-quality buses that it has been four days since they started running and their windows are breaking. (Technical Director, Operating Consultant)
Knowledge protection	Nondisclosure agreements	Nondisclosure agreement place restrictions on information sharing	We do nondisclosure agreement, that any type of pictures or any type of internet-based information should not be sent. Nobody can share information from their cell phone, laptop or desktop, not to themselves and not to others, so we have set these parameters for information leakage. (Communication Manager, Client)
	Standard operating procedures	Cameras are on a private network, not remotely accessible	You have to control leakages through SOPs. Our control room is very sensitive, in there is the surveillance feed, even our automatic fare collection and bus scheduling data comes at the portal. The cameras are on private network and are not remotely accessible, so in our contracts, there are specific clauses that the contractor cannot use any information without the client's permission. (Transport Manager, Client)

(continued)

**Table 2.** Continued

Themes	Subthemes	Initial coding	Illustrative quotes
	Education and training	Training, meetings and workshops to protect knowledge	<p>People are trained at various levels, there are meetings and workshops and conferences which are held in which the importance of protecting the specific or sensitive nature of knowledge is imparted, people are trained not to share anything that is sensitive or of sensitive nature or whose leakage may be detrimental for the project, for the organization or for the country. (Senior Project Manager, Design Consultant)</p>
	Sharing relevant knowledge	Information should not be shared with irrelevant people	<p>The information should not reach irrelevant people, whether the people are of your organization or outside, nobody should know the information about the organization who don't have any link with it, for example, my link is with operation and I should only know about, so what you have to do is that the information does not reach to people who are not relevant. (Communication Manager, Client)</p>

**Source(s):** Author's own work



**Figure 1.** Case study analysis process  
**Source:** Author's own work

Recently you have seen in [Newspaper name], it was published that [project's name of project] has removed hundreds of trees, but the question is that media does not know about the technicality. We have a policy that if we remove 1 tree, we plant 3 trees. However, the media depicts a very different picture. (Senior Manager, Client)

*Misuse of knowledge-sharing tools.* The misuse of both formal and informal knowledge-sharing tools is the main reason for knowledge leakage. As stated below:

One of our contactors shared information on LinkedIn. His company gave him an appreciation letter saying that you are working fine on this project. However, in that LinkedIn post he leaked some information which he should not have. (Transport Manager, Client)

Moreover, people involved in the project also leak information on social and electronic media. Sometimes, informal knowledge-sharing tools such as WhatsApp groups are used for knowledge leakage:

Before the project even started, the WhatsApp groups were made among the stakeholders then information sharing starts in that, so anyone can leak information. This was the case in [project's name], there was a progress review meeting and in that there were 40-50 people present, and when the meeting ended, the next day it is on Facebook, Media, Twitter or TV shows. (Technical Director, Operating Consultant)

*Diverse stakeholders' involvement.* There are different points in knowledge sharing, such that knowledge could get leaked from any one point. Letters, as the official mode of communication, are delivered by a mail carrier. They can get lost, or the carrier can open it and read the letter. As illustrated below:

We have a rider in all our offices, or we have a courier service, with whom we have a contract for monthly payments. A mail carrier comes to your office, picks up your courier and takes it away. You have made an envelope, it can be lost on the way, it could be misused. There are very few cases. But it happens sometimes. (Transport Manager, Client)

Moreover, sometimes there are wrong SOPs, which can lead to practices that are harmful and lead to knowledge leakage. As illustrated below:

---

There is a document called PC1. When the PC1 is approved by the [institute's name], they share your PC1 with every department [...] They ask you to print 50 copies of the PC1 and they share them with everyone, so it means they are sharing the knowledge with the contractors, they can easily get the copy and know the estimates, which is very dangerous. (Senior Manager, Client)

### *Knowledge protection*

*Nondisclosure agreements.* Knowledge protection can occur through nondisclosure agreements, which will clearly state that if an employee leaves the organization, he/she cannot disclose any information. As illustrated below:

We sign the non-disclosure agreement (NDA) with every employee. We sign 2 papers; one is contract and the other is NDA [...] by doing this our employees are legally covered with NDAs and the terms for that are that if you leave a project, you cannot share information for another one year. (Digital Marketing Manager, Digital Marketing Agency)

Moreover, organizations take certain steps to reduce knowledge leakage. For example, employees have to get approval from their department heads before leaving the organization; a condition can be imposed that an employee involved in a bidding process cannot leave the organization for a certain period of time. As stated below:

We deployed a strategy that any employee who is involved in the bidding process will first take permission of their department's head otherwise he can't leave the organization. The second is that when the bidding is in process, for six months. So, we imposed a condition on the employees' contract that till six months any employee who was involved in the bidding can't leave the organization. (Project Manager, Contractor 3)

NDAs are one way of preventing knowledge leakage from happening due to employee mobility.

*Standard operating procedures.* To protect knowledge from leakage, there are SOPs. These SOPs are implemented in different settings, for example, in the surveillance room. As illustrated below:

We have set up the SOP, the person watching the cameras will not use his personal phone. The company has given him a phone that is in the control room [...] their personal phones are submitted to our security office. The reason for that is that there are more than 600 cameras' feed playing on the screen and if there is something sensitive and they record it on their mobile, after that it can go anywhere. Now we do create SOPs you cannot plug in mouse, keyboard or USB, you can only view. (Transport Manager, Client)

In addition, encryption could also be used. Password encryption would also reduce knowledge leakage. However, there is a need to revisit SOPs. As stated below:

When the consultant makes any bill of quantity (BOQ), nowadays I ask them to give me in Excel but with a password. So, it is a password encrypted, and I am the only one who can see the document by putting the password [...] We should revisit our SOPs, starting with the email address, you should have a bar code card, QR-code card and your email should be of your company name not of Gmail. It should all be systematic and encrypted. (Senior Manager, Client)

Implementing SOPs could minimize knowledge leakage by avoiding information disorder and the misuse of knowledge-sharing tools.

*Education and training.* Organizations should provide training to protect knowledge. These training sessions contain information about what knowledge they could share and what they could not. As illustrated below:

Organizations hold regular training sessions. In general, there are circular advisories to all the people about the proper use of knowledge and when they are appointed, they are given this guideline that how do they handle these things and what is the proper professional, ethical behavior in this respect. (Senior Project Manager, Design Consultant)

Moreover, educating people who are using social media is very important. Anyone can use social media, but it is important to verify the source of information, not just to follow the trends. As stated below:

In my view, there is only one way that is to improve education, meaning we cannot shut down social media, and we cannot enforce it more than a certain level, it's just that who has the power of social media and he comes from an educational background [...] What I'm trying to say is if we do not mature the education system, the person posting on social media would not know that I should do research and get to know its pros and cons, its negatives, positives or its rights and wrongs. (Technical Director, Operating Consultant)

Education and training would reduce information disorder and the misuse of knowledge-sharing tools; as a result, knowledge leakage would be reduced.

*Sharing relevant knowledge.* Sharing relevant knowledge protects knowledge. In projects, all team members know their roles and responsibilities. The knowledge is shared with them that is relevant to performing their task. As illustrated below:

If there is a site engineer or a construction manager or a site supervisor, they know about their roles. They are only told about the directions and instructions which are related to their work. So, only concerned information is given out, only that is required. No extra information is given out ever. (Planning Engineer, Contractor 2)

Moreover, knowledge is shared in a controlled environment, with very few people having this knowledge. Through this approach, the knowledge could not be leaked. As stated below:

Information is shared in a very controlled environment like only 2-3 senior officers know about it and it is not spread forward in detail, we don't give it to the lower level and then you have to give controlled instructions. (Transport Manager, Client)

Sharing relevant knowledge would help to reduce knowledge leakage, particularly when diverse stakeholders are involved.

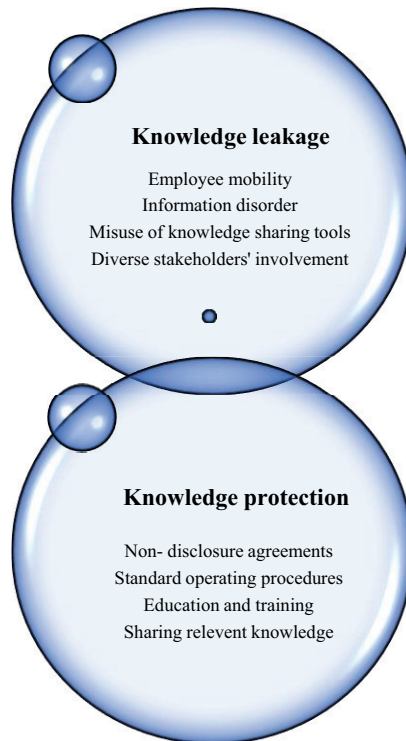
### Discussion

In interorganizational projects, cooperation – simultaneous cooperation and competition – emerges as organizations pursue shared goals while protecting their competitive interests (Bengtsson & Kock, 2014). Although such collaboration provides access to complementary resources and knowledge (Enberg, 2012; Gast et al., 2019), it also increases the risk of knowledge leakage, particularly among heterogeneous partners (Wang et al., 2024). Accordingly, organizations must protect their knowledge to sustain collaboration. This study examines knowledge leakage and protection (shown in Figure 2) using PMT, which conceptualizes leakage as a threat and protection as a coping response (Anderson & Agarwal, 2010; Rogers, 1975).

#### *Interorganizational knowledge leakage and protection*

The interorganizational knowledge leakage and protection matrix in Table 3 is based on the evidence from the findings.

Employee mobility is “the movement of employees into, within, and out of an organization” (Bibi, 2024: 4). There is an increase in employee mobility due to ongoing



**Figure 2.** Interorganizational knowledge leakage and protection framework

**Source:** Author's own work

technological, societal and economic changes (Mawdsley & Somaya, 2016). Employee mobility is essential to take into account with regard to knowledge leakage. Through employee mobility, organizations are able to access the critical knowledge that employees bring with them (Bibi, 2024; Franzoni, Scellato, & Stephan, 2018), which could lead to knowledge leakage, as shown in the findings. Moreover, the findings showed that nondisclosure agreements can protect knowledge leakages that occur due to employee mobility. A nondisclosure agreement is an “agreement restricting the use of information by prohibiting a contracting party from divulging data” (Beyer, 2001). A nondisclosure agreement is essentially a contractual incentive to ensure confidentiality and promote trust (Roth, 2023).

Media, including electronic, print and social media, has become a powerful tool to disseminate fake news. Fake news can have a significant impact on society as it has become easier to generate and harder to detect (Aimeur, Amri, & Brassard, 2023), which leads to information disorder. There are three types of information disorder: (i) misinformation is information that is false but not deliberately created to cause harm; (ii) disinformation is information that is false and intentionally created to harm individuals, social groups and organizations; and (iii) mal-information is based on reality and used to harm individuals and organizations (Wardle & Derakhshan, 2017). Moreover, interorganizational projects are multidisciplinary and interdependent on knowledge and skills. Hence, such projects make

**Table 3.** Interorganizational knowledge leakage and protection matrix

Knowledge protection	Knowledge leakage			
	Employee mobility	Information disorder	Misuse of knowledge sharing tools	Diverse stakeholders' involvement
Non-disclosure agreements	☀	⊘	⊘	⊘
Standard operating procedures	⊘	☀	☀	⊘
Education and training	⊘	☀	☀	⊘
Sharing relevant knowledge	⊘	⊘	⊘	☀

**Note:** ☀ = Relationship between knowledge leakage and knowledge protection; ⊘ = No relationship

**Source(s):** Author's own work

use of several tools, such as e-mail, WhatsApp, letters and meetings, to share knowledge (Iftikhar & Ahola, 2022). However, there are instances when these tools are used to share knowledge which should not be shared (Santos, Soares, & Carvalho, 2012). This is mainly due to an individual's deliberate misuse of knowledge-sharing tools. The findings presented evidence that knowledge leakage could happen due to information disorder and the misuse of knowledge-sharing tools. However, the findings also highlighted that SOPs and education and training could reduce information disorder and the misuse of knowledge-sharing tools. Standard operating procedures are defined "as written documents that indicate how to perform a routine or a task" (Freeman, Cook, & Hooijberg, 2021: 477). The provision of education and training develops or deepens and upgrades employees' skills (Klimplová, 2012).

A multi-stakeholder approach is used to execute and deliver interorganizational projects. Each stakeholder has their own responsibilities, requirements and objectives. Stakeholders can be members of a project's team, and depending on how they get engaged and what their roles are, they may have different interests, impacts and objectives for the project (Storvang & Clarke, 2014). The findings are consistent with those of Heravi, Coffey, & Trigunarsyah (2015), namely, that only certain groups may need to get fully involved in all phases of a project, otherwise the risk of knowledge leakage significantly increases. Moreover, in projects, team members assess the knowledge requirements and then deliver relevant knowledge or unique skills and know-how for performing tasks (Yoon, Kim, & Yun, 2024), which could also reduce knowledge leakage occurring due to multiple stakeholder involvement.

**Conclusion**

This paper addresses the following research questions: *How does knowledge leakage occur in an interorganizational project?* and *How do organizations protect knowledge in an*

---

*interorganizational project?* It provides a comprehensive understanding of the leakage and protection of knowledge within an interorganizational context. The study identifies key causes of knowledge leakage – such as employee mobility, information disorder, misuse of knowledge-sharing tools and diverse stakeholder involvement – and explores protection mechanisms including nondisclosure agreements, SOPs, education and training and selective knowledge sharing.

### *Theoretical implications*

This study makes significant theoretical contributions. First, it deepens understanding of how knowledge leakage and protection operate in complex interorganizational environments where multiple organizations collaborate. Second, drawing on PMT, it clarifies the relationship between threat and coping mechanisms: knowledge leakage, such as employee mobility, acts as a threat, while protective practices – such as nondisclosure agreements – serve as coping responses to the project and the organization. Third, the interplay between knowledge leakage and knowledge protection practices is the focus of critical findings, as delineated in [Table 3](#). This interplay not only elucidates the causes of knowledge leakage but also offers evidence regarding the potential for knowledge protection in initiatives to address knowledge leakage. Finally, the proposed framework ([Figure 2](#)) offers a foundation for future research on the unique dynamics of knowledge leakage and protection in interorganizational projects.

### *Practical implications*

There are certain practical implications. First, this study will assist managers and organizations in thinking through the reasons behind knowledge leakage, allowing them to avoid conditions and events that increase knowledge leakage by introducing systems such as digital governance. Second, knowledge protection is appealing to managers and organizations because they can implement policies and foster a trust culture and environment in which relevant knowledge can be shared and valued. Third, the matrix ([Table 3](#)) advises project participants and organizations on how to safeguard knowledge and reduce knowledge leakage; this enables project practitioners to have a better understanding of knowledge leakage and protection.

### *Limitations and future research areas*

It is essential to acknowledge the limitations. First, from an internal validity point of view, we analyzed interview data and provided details about data analysis. It has been challenging to combine different views from interviews and display them in the findings. This approach helped to validate the findings, but there are personal biases involved in qualitative research. Second, from an external validity point of view ([Miles, Huberman, & Saldaña, 2014; Yin, 2018](#)), the study can be replicated in other contexts with some similarities and differences.

This study opens several avenues for further research. First, a single case study is considered; we believe that our findings are transferable beyond interorganizational projects since data is collected from a heterogeneous set of organizations. Future research may undertake a comparative study to explore knowledge hiding in different types of infrastructural projects and industries. Second, the evidence from the data did not identify the different levels (individual, team and organization) at which knowledge leakage and protection occur. Future research should provide a dedicated examination of knowledge leakage and protection at different levels. Third, the study was conducted in Pakistan. Research in the context of other national backgrounds is required to verify the findings. Fourth, the study is cross-sectional. Longitudinal studies should also be used in future

research. Fifth, the analysis is done solely by the lead author with debriefings; however, qualitative research is subjective in nature, and the researcher's interests might have an impact on the study. Finally, due to the travel restrictions associated with COVID-19, interviews were conducted on MS Teams. Hence, there is a possibility that some good potential interviewees may have been missing.

## References

- Ahlfänger, M., Gemünden, H. G., & Leker, S. (2022). Balancing knowledge sharing with protecting: The efficacy of formal control in open innovation projects. *International Journal of Project Management*, 40(2), 105-119, <https://doi.org/10.1016/j.ijproman.2021.09.007>.
- Aimeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: A review. *Social Network Analysis and Mining*, 13(1), 30, <https://doi.org/10.1007/s13278-023-01028-5>.
- Andersén, J. (2012). Protective capacity and absorptive capacity: Managing the balance between retention and creation of knowledge-based resources. *The Learning Organization*, 19(5), 440-452, <https://doi.org/10.1108/09696471211239730>.
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-643, <https://doi.org/10.2307/25750694>.
- Argote, L., McEvily, B., & Reagans, R. (2003). Managing knowledge in organizations: An integrative framework and review of emerging themes. *Management Science*, 49(4), 571-582, <https://doi.org/10.1287/mnsc.49.4.571.14424>.
- Arias-Pérez, J., Lozada, N., & Henao-García, E. (2020). When it comes to the impact of absorptive capacity on co-innovation, how really harmful is knowledge leakage? *Journal of Knowledge Management*, 24(8), 1841-1857, <https://doi.org/10.1108/JKM-02-2020-0084>.
- Balle, A. R., Steffen, M. O., Curado, C., & Oliveira, M. (2019). Interorganizational knowledge sharing in a science and technology park: The use of knowledge sharing mechanisms. *Journal of Knowledge Management*, 23(10), 2016-2038, <https://doi.org/10.1108/JKM-05-2018-0328>.
- Barringer, B. R., & Harrison, J. S. (2000). Walking a tightrope: Creating value through interorganizational relationships. *Journal of Management*, 26(3), 367-403, [https://doi.org/10.1016/S0149-2063\(00\)00046-5](https://doi.org/10.1016/S0149-2063(00)00046-5).
- Bengtsson, M., & Kock, S. (2014). Coopetition – quo Vadis? Past accomplishments and future challenges. *Industrial Marketing Management*, 43(2), 180-188, <https://doi.org/10.1016/j.indmarman.2014.02.015>.
- Beyer, G. W. (2001). *Modern dictionary for the legal profession* (3rd ed.), William S. Hein & Co.
- Bibi, G. (2024). Employee mobility as a knowledge development strategy. *Human Resource Management Review*, 34(2), 101014, <https://doi.org/10.1016/j.hrmr.2024.101014>.
- Bloodgood, J. M., & Chen, A. N. K. (2022). Preventing organizational knowledge leakage: The influence of knowledge seekers' awareness, motivation and capability. *Journal of Knowledge Management*, 26(9), 2145-2176, <https://doi.org/10.1108/JKM-12-2020-0894>.
- Braun, T., & Sydow, J. (2019). Selecting organizational partners for interorganizational projects: The dual but limited role of digital capabilities in the construction industry. *Project Management Journal*, 50(4), 398-408, <https://doi.org/10.1177/8756972819857477>.
- Braun, V., & Clarke, V. (2012). Thematic analysis, in Cooper, H., Camic, P.M., Long, D.L., Panter, A.T., Rindskopf, D., Sher, K.J., *APA handbook of research methods in psychology: Research designs: Quantitative, qualitative, neuropsychological, and biological*, American Psychological Association, 57-71.

- Carmel, J., Pak, Y., & Patel, K. (2013). Knowledge loss when older experts leave knowledge-intensive organisations. *Journal of Knowledge Management*, 17(6), 913-927, <https://doi.org/10.1108/JKM-04-2013-0137>.
- Chalkiti, K., & Sigala, M. (2010). Staff turnover in the Greek tourism industry: A comparison between insular and peninsular regions. *International Journal of Contemporary Hospitality Management*, 22(3), 335-359, <https://doi.org/10.1108/0959611011035945>.
- Chan, P. C. W., & Lee, W. B. (2011). Knowledge audit with intellectual capital in the quality management process: An empirical study in an electronics company. *The Electronic Journal of Knowledge Management*, 9(2), 98-116.
- Charterina, J., Basterretxea, I., & Landeta, J. (2017). Collaborative relationships with customers: Generation and protection of innovations. *Journal of Business & Industrial Marketing*, 32(5), 733-741, <https://doi.org/10.1108/JBIM-02-2017-0052>.
- Chen, H., Yao, Y., Zan, A., & Carayannis, E. G. (2021). How does coepetition affect radical innovation? The roles of internal knowledge structure and external knowledge integration. *Journal of Business & Industrial Marketing*, 36(11), 1975-1987, <https://doi.org/10.1108/JBIM-05-2019-0257>.
- Das, T. K., & Teng, B. S. (2001). A risk perception model of alliance structuring. *Journal of International Management*, 7(1), 1-29, [https://doi.org/10.1016/S1075-4253\(00\)00037-5](https://doi.org/10.1016/S1075-4253(00)00037-5).
- de Faria, P., & Sofka, W. (2010). Knowledge protection strategies of multinational firms – a cross-country comparison. *Research Policy*, 39(7), 956-968, <https://doi.org/10.1016/j.respol.2010.03.005>.
- DeSouza, K. C. (2006). Knowledge security: An interesting research space. *Journal of Information Science and Technology*, 3(1), 1-7.
- Durst, S., Aggestam, L., & Ferenhof, H. A. (2015). Understanding knowledge leakage: A review of previous studies. *Vine*, 45(4), 568-586, <https://doi.org/10.1108/VINE-01-2015-0009>.
- Easterby-Smith, M., Lyles, M. A., & Tsang, E. W. K. (2008). Inter-organizational knowledge transfer: Current themes and future prospects. *Journal of Management Studies*, 45(4), 677-690, <https://doi.org/10.1111/j.1467-6486.2008.00773.x>.
- Enberg, C. (2012). Enabling knowledge integration in coepetitive R&D projects: The management of conflicting logics. *International Journal of Project Management*, 30(7), 771-780, <https://doi.org/10.1016/j.ijproman.2012.01.003>.
- Estrada, I., Faems, D., & de Faria, P. (2016). Coepetition and product innovation performance: The role of internal knowledge sharing mechanisms and formal knowledge protection mechanisms. *Industrial Marketing Management*, 53(1), 56-65, <https://doi.org/10.1016/j.indmarman.2015.11.013>.
- Fernandes, E. B., Wegner, D., & Möllering, G. (2023). Governance of interorganizational projects: A process-based approach applied to a Latin American–European case. *Project Management Journal*, 54(3), 219-234, <https://doi.org/10.1177/87569728221145927>.
- Fernandez, A.-S., & Chiambaretto, P. (2016). Managing tensions related to information in coepetition. *Industrial Marketing Management*, 53(1), 66-76, <https://doi.org/10.1016/j.indmarman.2015.11.010>.
- Flammer, C., & Kacperczyk, A. (2019). Corporate social responsibility as a defense against knowledge spillovers: Evidence from the inevitable disclosure doctrine. *Strategic Management Journal*, 40(8), 1243-1267, <https://doi.org/10.1002/smj.3025>.
- Franzoni, C., Scellato, G., & Stephan, P. (2018). Context factors and the performance of mobile individuals in research teams. *Journal of Management Studies*, 55(1), 27-59, <https://doi.org/10.1111/joms.12279>.
- Freeman, K. P., Cook, J. R., & Hooijberg, E. H. (2021). Standard operating procedures. *Journal of the American Veterinary Medical Association*, 258(5), 477-481, <https://doi.org/10.2460/javma.258.5.477>.
- Frishammar, J., Ericsson, K., & Patel, P. C. (2015). The dark side of knowledge transfer: Exploring knowledge leakage in joint R&D projects. *Technovation*, 41-42, 75-88, <https://doi.org/10.1016/j.technovation.2015.01.001>.

- Gast, J., Gundolf, K., Harms, R., & Collado, E. M. (2019). Knowledge management and cooperation: How do cooperating competitors balance the needs to share and protect their knowledge? *Industrial Marketing Management*, 77, 65-74, <https://doi.org/10.1016/j.indmarman.2018.12.007>.
- Grillitsch, M., & Nilsson, M. (2017). Firm performance in the periphery: On the relation between firm-internal knowledge and local knowledge spillovers. *Regional Studies*, 51(8), 1219-1231, <https://doi.org/10.1080/00343404.2016.1175554>.
- Hamel, G. (1991). Competition for competence and inter-partner learning within international strategic alliances. *Strategic Management Journal*, 12(S1), 83-104, <https://doi.org/10.1002/smj.4250120908>.
- Hamel, G., Doz, Y. L., & Prahalad, C. K. (1989). Collaborate with your competitors and win. *Harvard Business Review*, 67(1), 133-139.
- Hartley, J. (2004). Case study research, in Cassell, C. & Symon, G. (Eds), *Essential guide to qualitative methods in organizational research*, Sage, 323-333.
- Heiman, B. A., & Nickerson, J. A. (2004). Empirical evidence regarding the tension between knowledge sharing and knowledge expropriation in collaborations. *Managerial and Decision Economics*, 25(6-7), 401-420, <https://doi.org/10.1002/mde.1198>.
- Heravi, A., Coffey, V., & Trigunaryyah, B. (2015). Evaluating the level of stakeholder involvement during the project planning processes of building projects. *International Journal of Project Management*, 33(5), 985-997, <https://doi.org/10.1016/j.ijproman.2014.12.007>.
- Hernandez, E., Sanders, W. M. G., & Tuschke, A. (2015). Network defense: Pruning, grafting, and closing to prevent leakage of strategic knowledge to rivals. *Academy of Management Journal*, 58(4), 1233-1260, <https://doi.org/10.5465/amj.2012.0773>.
- Howitt, D., & Cramer, D. (2007). *Introduction to research methods in psychology*, Pearson Education.
- Iftikhar, R., & Ahola, T. (2022). Knowledge sharing in an interorganizational setting: Empirical evidence from the orange line metro train project. *Journal of Knowledge Management*, 26(4), 854-872, <https://doi.org/10.1108/JKM-06-2020-0485>.
- Jaffe, A., Trajtenberg, M., & Henderson, R. (1993). Geographic localization of knowledge spillovers as evidenced by patent citations. *The Quarterly Journal of Economics*, 108(3), 577-598, <https://doi.org/10.2307/2118401>.
- James, S. D., Leiblein, M. J., & Lu, S. (2013). How firms capture value from their innovations. *Journal of Management*, 39(5), 1123-1155, <https://doi.org/10.1177/0149206313488211>.
- Jiang, X., Bao, Y., Xie, Y., & Gao, S. (2016). Partner trustworthiness, knowledge flow in strategic alliances, and firm competitiveness: A contingency perspective. *Journal of Business Research*, 69(2), 804-814, <https://doi.org/10.1016/j.jbusres.2015.07.009>.
- Jiang, X., Li, M., Gao, S., Bao, Y., & Jiang, F. (2013). Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. *Industrial Marketing Management*, 42(6), 983-991, <https://doi.org/10.1016/j.indmarman.2013.03.013>.
- Kale, P., Singh, H., & Perlmutter, H. (2000). Learning and protection of proprietary assets in strategic alliances: Building relational capital. *Strategic Management Journal*, 21(3), 217-237, [https://doi.org/10.1002/\(SICI\)1097-0266\(200003\)21:3%3C217::AID-SMJ95%3E3.0.CO;2-Y](https://doi.org/10.1002/(SICI)1097-0266(200003)21:3%3C217::AID-SMJ95%3E3.0.CO;2-Y).
- Klímplová, L. (2012). Employers' view on problems related to workforce skills and qualification. *Journal of Competitiveness*, 4, 50-66, <https://doi.org/10.7441/joc.2012.04.04>.
- Lado, A. A., Boyd, N. G., & Hanlon, S. C. (1997). Competition, cooperation, and the search for economic rents: A synthetic model. *The Academy of Management Review*, 22(1), 110-141, <https://doi.org/10.5465/amr.1997.9707180261>.
- Lee, S. C., Chang, S. N., Liu, C. Y., & Yang, J. (2007). The effect of knowledge protection, knowledge ambiguity, and relational capital on alliance performance. *Knowledge and Process Management*, 14(1), 58-69, <https://doi.org/10.1002/kpm.270>.

- Leiponen, A., & Byma, J. (2009). If you cannot block, you better run: Small firms, cooperative innovation, and appropriation strategies. *Research Policy*, 38(9), 1478-1488, <https://doi.org/10.1016/j.respol.2009.06.003>.
- Li, Y., Liu, Y., & Liu, H. (2011). Co-opetition, distributor's entrepreneurial orientation and manufacturer's knowledge acquisition: Evidence from China. *Journal of Operations Management*, 29(1-2), 128-142, <https://doi.org/10.1016/j.jom.2010.07.006>.
- Love, J. H., Roper, S., & Vahter, P. (2014). Learning from openness: The dynamics of breadth in external innovation linkages. *Strategic Management Journal*, 35(11), 1703-1716, <https://doi.org/10.1002/smj.2170>.
- Lumineau, F., & Oliveira, N. (2018). A pluralistic perspective to overcome major blind spots in research on interorganizational relationships. *Academy of Management Annals*, 12(1), 440-465, <https://doi.org/10.5465/annals.2016.0033>.
- Magni, D., Chierici, R., Fait, M., & Lefebvre, K. (2022). A network model approach to enhance knowledge sharing for internationalization readiness of SMEs. *International Marketing Review*, 39(3), 626-652, <https://doi.org/10.1108/IMR-03-2021-0110>.
- Malhotra, D., & Murnighan, J. K. (2002). The effects of contracts on interpersonal trust. *Administrative Science Quarterly*, 47(3), 534-559, <https://doi.org/10.2307/3094850>.
- Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: A structured literature review. *Journal of Knowledge Management*, 19(2), 190-211, <https://doi.org/10.1108/JKM-05-2014-0198>.
- Manning, S. (2017). The rise of project network organizations: Building core teams and flexible partner pools for interorganizational projects. *Research Policy*, 46(8), 1399-1415, <https://doi.org/10.1016/j.respol.2017.06.005>.
- Matusik, S. F., & Hill, C. W. L. (1998). The utilization of contingent work, knowledge creation, and competitive advantage. *The Academy of Management Review*, 23(4), 680-697, <https://doi.org/10.2307/259057>.
- Mawdsley, J. K., & Somaya, D. (2016). Employee mobility and organizational outcomes: An integrative conceptual framework and research agenda. *Journal of Management*, 42(1), 85-113, <https://doi.org/10.1177/0149206315616459>.
- Miles, M. B., Huberman, M. A., & Saldaña, J. (2014). *Qualitative data analysis: a methods sourcebook*, Sage Publications.
- Mohr, J. J., & Sengupta, S. (2002). Managing the paradox of inter-firm learning: The role of governance mechanisms. *Journal of Business & Industrial Marketing*, 17(4), 282-301, <https://doi.org/10.1108/08858620210431688>.
- Nelson, R. R., & Winter, S. G. (1982). *An evolutionary theory of economic change*, Harvard University Press.
- Nonaka, I., & Von Krogh, G. (2009). Tacit knowledge and knowledge conversion: Controversy and advancement in organizational knowledge creation theory. *Organization Science*, 20(3), 635-652, <https://doi.org/10.1287/orsc.1080.0412>.
- Olander, H., Vanhala, M., & Hurmelinna-Laukkanen, P. (2014). Reasons for choosing mechanisms to protect knowledge and innovations. *Management Decision*, 52(2), 207-229, <https://doi.org/10.1108/MD-11-2012-0791>.
- Oliveira, N., & Lumineau, F. (2017). How coordination trajectories influence the performance of interorganizational project networks. *Organization Science*, 28(6), 1029-1060, <https://doi.org/10.1287/orsc.2017.1151>.
- Rippeto, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, 52(3), 596-604, <https://doi.org/10.1037//0022-3514.52.3.596>.
- Ritala, P., Kenneth, H., Heidi, O., & Snejdina, M. (2018). External knowledge sharing and radical innovation: The downsides of uncontrolled openness. *Journal of Knowledge Management*, 22(5), 1104-1123, <https://doi.org/10.1108/JKM-05-2017-0172>.

- Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation*, 35, 22-31, <https://doi.org/10.1016/j.technovation.2014.07.011>.
- Ritala, P., Kianto, A., Vanhala, M., & Hussinki, H. (2023). To protect or not to protect? Renewal capital, knowledge protection and innovation performance. *Journal of Knowledge Management*, 27(11), 1-24, <https://doi.org/10.1108/JKM-11-2021-0866>.
- Ritala, P., & Hurmelinna-Laukkanen, P. (2013). Incremental and radical innovation in coopetition – the role of absorptive capacity and appropriability. *Journal of Product Innovation Management*, 30(1), 154-169, <https://doi.org/10.1111/j.1540-5885.2012.00956.x>.
- Roehrich, J. K., Kalra, J., Squire, B., & Davies, A. (2023). Network orchestration in a large inter-organizational project. *Journal of Operations Management*, 69(7), 1078-1099, <https://doi.org/10.1002/joom.1237>.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114, <https://doi.org/10.1080/00223980.1975.9915803>.
- Roth, D. (2023). NDAs: how should Christians think about non-disclosure agreements? In all things. Retrieved from [https://digitalcollections.dordt.edu/cgi/viewcontent.cgi?article=2468&context=faculty\\_work](https://digitalcollections.dordt.edu/cgi/viewcontent.cgi?article=2468&context=faculty_work)
- Santos, V. R., Soares, A. L., & Carvalho, J. Á. (2012). Knowledge sharing barriers in complex research and development projects: An exploratory study on the perceptions of project managers. *Knowledge and Process Management*, 19(1), 27-38, <https://doi.org/10.1002/kpm.1379>.
- Sharif, S. M. F., Naiding, Y., Xu, Y., & Rehman, A. U. (2020). The effect of contract completeness on knowledge leakages in collaborative construction projects: A moderated mediation study. *Journal of Knowledge Management*, 24(9), 2057-2078, <https://doi.org/10.1108/JKM-04-2020-0322>.
- Shi, X., Zhang, Q., & Zheng, Z. (2019). The double-edged sword of external search in collaboration networks: Embeddedness in knowledge networks as moderators. *Journal of Knowledge Management*, 23(10), 2135-2160, <https://doi.org/10.1108/JKM-04-2018-0226>.
- Shujahat, M., Sousa, M. J., Hussain, S., Nawaz, F., Wang, M., & Umer, M. (2017). Translating the impact of knowledge management processes into knowledge-based innovation: The neglected and mediating role of knowledge-worker productivity. *Journal of Business Research*, 94, 442-450, <https://doi.org/10.1016/j.jbusres.2017.11.001>.
- Silva, M. D., Howell, J., & Meyer, M. (2018). Innovation intermediaries and collaboration: Knowledge-based practices and internal value creation. *Research Policy*, 47(1), 70-87, <https://doi.org/10.1016/j.respol.2017.09.011>.
- Solli-Sæther, H., Karlsen, J. T., & van Oorschot, K. (2015). Strategic and cultural misalignment: Knowledge sharing barriers in project networks. *Project Management Journal*, 46(3), 49-60, <https://doi.org/10.1002/pmj.21501>.
- Somaya, D. (2003). Strategic determinants of decisions not to settle patent litigation. *Strategic Management Journal*, 24(1), 17-38, <https://doi.org/10.1002/smj.281>.
- Spender, J. C. (1996). Making knowledge the basis of a dynamic theory of the firm. *Strategic Management Journal*, 17(S2), 45-62, <https://doi.org/10.1002/smj.4250171106>.
- Storvang, P., & Clarke, A. H. (2014). How to create a space for stakeholders' involvement in construction. *Construction Management and Economics*, 32(12), 1166-1182, <https://doi.org/10.1080/01446193.2014.966732>.
- Thomä, J., & Bizer, K. (2013). To protect or not to protect? Modes of appropriability in the small enterprise sector. *Research Policy*, 42(1), 35-49, <https://doi.org/10.1016/j.respol.2012.04.019>.
- Tiwana, A. (2008). Does interfirm modularity complement ignorance? A field study of software outsourcing alliances. *Strategic Management Journal*, 29(11), 1241-1252, <https://doi.org/10.1002/smj.694>.
- Treleaven, L., & Sykes, C. (2005). Loss of organizational knowledge: From supporting clients to serving head office. *Journal of Organizational Change Management*, 18(4), 353-368, <https://doi.org/10.1108/09534810510607056>.

- Walter, S. G., Walter, A., & Müller, D. (2015). Formalization, communication quality, and opportunistic behavior in R&D alliances between competitors. *Journal of Product Innovation Management*, 32(6), 954-970, <https://doi.org/10.1111/jpim.12209>.
- Wang, C., Chin, T., Chiew, Y. Y., & Capalbo, C. (2024). How geographic diversity and collaborative breadth prevent knowledge leakage during open innovation processes. *Journal of Knowledge Management*, 28(3), 743-762, <https://doi.org/10.1108/JKM-04-2022-0298>.
- Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. *Council of Europe Report*, 27, 1-107.
- Wu, L.-W., & Lin, J.-R. (2013). Knowledge sharing and knowledge effectiveness: learning orientation and co-production in the contingency model of tacit knowledge. *Journal of Business & Industrial Marketing*, 28(8), 672-686, <https://doi.org/10.1108/JBIM-04-2011-0050>.
- Yahav, I., Schwartz, D. G., & Silverman, G. (2014). Detecting unintentional information leakage in social media news comments. *Proceedings of IEEE 15th International Conference on Information Reuse and Integration*, 74-79.
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.), Sage Publications, Incorporated.
- Yoon, S., Kim, S. L., & Yun, S. (2024). Supervisor knowledge sharing and creative behavior: The roles of employees' self-efficacy and work-family conflict. *Journal of Management & Organization*, 30(6), 1920-1935, <https://doi.org/10.1017/jmo.2022.85>.

## Appendix. Interview guide

### *Background information:*

- Could you please tell me about your role and responsibilities in this project?
- How long have you been working on this project or with this organization?

### *Knowledge leakage:*

- Have you experienced knowledge leakage?
- How does knowledge leakage occur?
- Does your organization have any formal or informal routines for dealing with (potential) knowledge leakage? Please explain

### *Knowledge protection:*

- How do you currently share sensitive knowledge among employees, partners and clients?
- How do you decide this knowledge should be shared? And how much should be shared?
- What current mechanisms do you use to protect *Knowledge*?
- How to facilitate knowledge protection within individuals, teams, organizations and across organizations?
- Would you like to add anything further?

## Corresponding author

Rehab Iftikhar can be contacted at: [rehab.iftikhar@uws.ac.uk](mailto:rehab.iftikhar@uws.ac.uk)